DigitalSign 5.0

Guida Utente

Sommario

1 Generalità e Concetti 5

1.1 Principi e riferimenti normativi sulle firme elettroniche 5
1.1.1 Concetti di “firma elettronica”, “firma elettronica avanzata”, “firma digitale”, “firma elettronica qualificata” 5
1.1.2 La tecnologia della firma digitale 5
1.1.3 Il certificato di chiave pubblica 6
1.1.4 Il Certificatore 7
1.1.5 Le liste di Sospensione e Revoca 7
1.1.6 Il processo di verifica di una firma digitale 8
1.1.7 Le Marche Temporali (*Timestamp*) 9
1.1.8 I formati di rappresentazione dei documenti firmati 9

2 Installazione e registrazione 11

2.1 La procedura di installazione 11
2.1.1 L’installazione “silente” 13

2.2 Registrazione ed Attivazione 13
2.2.1 Registrazione off-line: modalità XML 16
2.2.2 Registrazione off-line: modalità manuale 19

3 Riferimento 21

3.1 DigitalSign sullo schermo 21
3.1.1 La finestra principale 21
3.1.2 La finestra documento 22
3.1.2.1 Documenti di tipo CAdES 22
3.1.2.2 Documenti di tipo PAdES 23
3.1.2.3 Finestra documento: area “Proprietà” 24
3.1.2.4 Finestra documento: area “Dettagli” 27
3.1.3 La barra menu di DigitalSign 27
3.1.4 Le barre strumenti *(toolbar)* 28
3.1.5 I Pannelli Informativi 28
3.1.6 La barra di stato 30

3.2 Il menu “File” 30
3.2.1 Log On / Log Off 31
3.2.2 Controllo licenze 31
3.2.3 Il sottomenu “Apri” 32
3.2.3.1 Documento 32
3.2.3.2 Visualizza certificato 32
3.2.3.3 Visualizza Richiesta di Certificato 32
3.2.3.4 Visualizza CRL 32
3.2.4 Salva Documento 32
3.2.5 Salva Documento con Nome 33
3.2.6 Salva Contenuto 33
3.2.7 Elaborazione Automatica 34
3.2.7.1 Firma CAdES 35
3.2.7.2 Firma PAdES 37
3.2.7.3 Verifica 38
3.2.7.4 Marcatura Temporale 38
3.2.7.5 Controfirma 39
3.2.7.6 Cifratura 40
3.2.7.7 Decifratura 40
3.2.8 Stampa 40
3.2.9 Genera Report 41
3.2.10 Il sottomenu “Invia Email” 41
3.2.11 Registro Attività 42
3.2.12 Uscita 42

3.3 Il menu “Strumenti” 43
3.3.1 Richiesta di certificato PKCS#10 43
3.3.2 Gestione DB Locale dei Certificati 43

3.3.3 Gestione CRL ... 44
3.3.4 Opzioni di Security ... 44
3.3.5 Opzioni ... 44
3.3.6 Il sottomenu “Configurazione Servizi” ... 44
3.3.7 Personal Certification Authority ... 44

3.4 Il menu “Dispositivo di Firma” ... 44
3.4.1 Gestione Chiavi RSA ... 45
3.4.2 Gestione Certificati ‘on-board’ ... 45
3.4.3 Configurazione ... 45
3.4.4 Informazioni sul Dispositivo ... 45

3.5 Il menu “Documento” ... 46
3.5.1 Aggiungi Firma CAdES ... 46
3.5.2 Aggiungi Firma PDF ... 48
3.5.3 Aggiungi Firma Grafometrica ... 53
3.5.4 Marca Temporale ... 53
3.5.5 Destinatario Cifratura ... 54
3.5.6 Annulla Tutto ... 56
3.5.7 Wipe File ... 56
3.5.8 Verifica alla data ... 57
3.5.9 Sottomenu Modalità Visualizzazione ... 57
3.5.10 Sottomenu Securview ASCIII/RTF ... 58
3.5.11 Sottomenu Securview Imaging ... 58

3.6 Il menu “Finestre” ... 59
3.6.1 Mostra pannelli di informazione ... 60

3.7 Il menu “Aiuto” ... 60
3.7.1 Documentazione ... 60
3.7.2 Mostra Licenza d’uso ... 60
3.7.3 Procedura di Registrazione ... 61
3.7.4 Attivazione ... 61
3.7.5 Disattivazione ... 61
3.7.6 Informazioni su DigitalSign ... 61

3.8 Moduli di gestione e finestre di dialogo ... 62
3.8.1 Logon al dispositivo di firma ... 63
3.8.2 Modulo di gestione del DB dei Certificati ... 63
3.8.3 Modulo di Gestione delle Liste di Sospensione e Revoca (CRL) ... 65
3.8.4 Modulo di Gestione delle Opzioni di Security ... 66
3.8.4.1 Firma e verifica ... 67
3.8.4.2 CA accreditate/attendibili ... 69
3.8.4.3 Operazioni su file da interfaccia COM ... 70
3.8.5 Modulo di Gestione delle Opzioni ... 71
3.8.5.1 Generali ... 71
3.8.5.2 ActiveDocument ... 73
3.8.5.3 Testo e “Rich Text” ... 73
3.8.5.4 Esadecimale ... 74
3.8.5.5 Percorsi ... 75
3.8.5.6 Toolbar ... 76
3.8.5.7 Registrazione Eventi ... 77
3.8.5.8 Associazioni ... 78
3.8.5.9 Configurazione Internet ... 78
3.8.5.10 COM Add-Ins ... 79
3.8.6 Modulo di Configurazione dei servizi di accesso agli elenchi di certificati LDAP ... 80
3.8.6.1 Finestra di configurazione di un servizio LDAP ... 80
3.8.7 Modulo di Configurazione dei servizi di Marcatura Temporale ... 81
3.8.7.1 Finestra di configurazione per un account di Marcatura Temporale ... 82
3.8.8 Modulo per la generazione di una CRL ... 83
3.8.9 Modulo di visualizzazione di un Certificato ... 85
3.8.10 Modulo di visualizzazione di una Lista di Sospensione o Revoca ... 87
3.8.11 Modulo di gestione delle coppie di chiavi RSA ... 89
3.8.11.1 Proprietà di una coppia di chiavi ... 90

3.8.12 Modulo di Gestione dei Certificati 'on-board' 90
3.8.13 Modulo di Gestione della Configurazione del Dispositivo di Firma 91
3.8.13.1 Auto-configurazione 91
3.8.13.2 Configurazione manuale 92
3.8.13.3 Aggiunta di un Profilo di Configurazione 93
3.8.13.4 Diagnostica del dispositivo 94
3.8.13.5 Caricamento file PKCS#12 95
3.8.14 Verifica alla Data 97
3.8.14.1 Verifica di documenti marcati temporalmente 98

3.9 Appendici 99
3.9.1 Interfacciamento dei dispositivi di firma 99
3.9.2 Marche temporali: contenuto e modalità di associazione ai documenti 100
3.9.3 La cifratura dei contenuti in DigitalSign 102
3.9.4 Firma semiautomatica dalla *shell* di Windows 103

1 Generalità e Concetti

1.1 Principi e riferimenti normativi sulle firme elettroniche

1.1.1 Concetti di "firma elettronica", "firma elettronica avanzata", "firma digitale", "firma elettronica qualificata"

Una definizione di **firma elettronica**, tratta dalla Direttiva Comunitaria 1999/93/CE e ripresa dal nostro Codice dell'Amministrazione Digitale, è la seguente:

"un insieme di dati in forma elettronica, allegati o logicamente associati con altri dati elettronici e che servono come metodo di autenticazione".

Si tratta evidentemente di una definizione assai generale, in cui ricade un vasto spettro di strumenti. Anche scrivere il proprio nome in calce ad un messaggio email può essere considerato una forma di firma elettronica.

La normativa distingue poi diverse fattispecie di firma elettronica:
- **Firma Elettronica Avanzata**
- **Firma Digitale**
- **Firma Elettronica Qualificata**

Mentre nell'attuale (2014) formulazione delle norme la **firma digitale** e la **firma qualificata** sono pressoché coincidenti (certamente non esistono sul mercato soluzioni distinte per le due tipologie), la firma elettronica avanzata (di cui – ricordiamo – la firma qualificata è un caso particolare) è una fattispecie più ampia, che si apre a diverse interpretazioni.

In particolare, per quello che riguarda gli utenti di DigitalSign:
- La **Firma Grafometrica**, se adeguatamente supportata da un processo conforme alle Regole Tecniche, può assumere la dignità di Firma Elettronica Avanzata. Se invece il processo che supporta la raccolta di questo tipo di firma è incompleto, allora si decade al rango di **firma elettronica semplice**.
- La firma apposta con il certificato di autenticazione contenuto in una CNS (Carta Nazionale dei Servizi), se rivolta alla Pubblica Amministrazione è a tutti gli effetti una **Firma Elettronica Avanzata**. Resta una **firma elettronica semplice** negli altri casi.

Si noti che tutte le tipologie di firma menzionate sono riconducibili al caso di una firma elettronica basata su una coppia di chiavi ed un certificato, come vedremo nelle prossime sezioni. Anche il caso della firma grafometrica, basata sulla raccolta di dati biometrici da parte di un tablet sensibile, usa la tecnologia della firma digitale per collegare univocamente i dati biometrici al contenuto del documento mediante una coppia di chiavi ed un certificato.

1.1.2 La tecnologia della firma digitale

Mentre la normativa italiana assegna all'espressione "firma digitale" un particolare significato giuridico conseguente all'adozione di vincoli importanti, in termini tecnologici la digital signature è *"un particolare tipo di firma elettronica basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare provenienza e integrità di un documento informatico"*

In altre parole, con "firma digitale" si intende di regola un particolare tipo di "firma elettronica", realizzata mediante l'uso di algoritmi di *hashing* per derivare un'impronta dai dati oggetto della firma, e da algoritmi di crittografia asimmetrica per derivare la firma dall'impronta.

Le due chiavi di una coppia vengono gestite in modo che la chiave privata resti in totale ed esclusiva disponibilità del sottoscrittore, e che la chiave pubblica sia effettivamente accessibile a chiunque si trovi nella necessità di verificare una firma.

Per rendere la chiave pubblica effettivamente fruibile e per associare la coppia di chiavi ad una identità, si adotta lo strumento del certificato di chiave pubblica (si veda la prossima sezione).

Questa tecnica soddisfa i requisiti delle firme elettroniche perché:

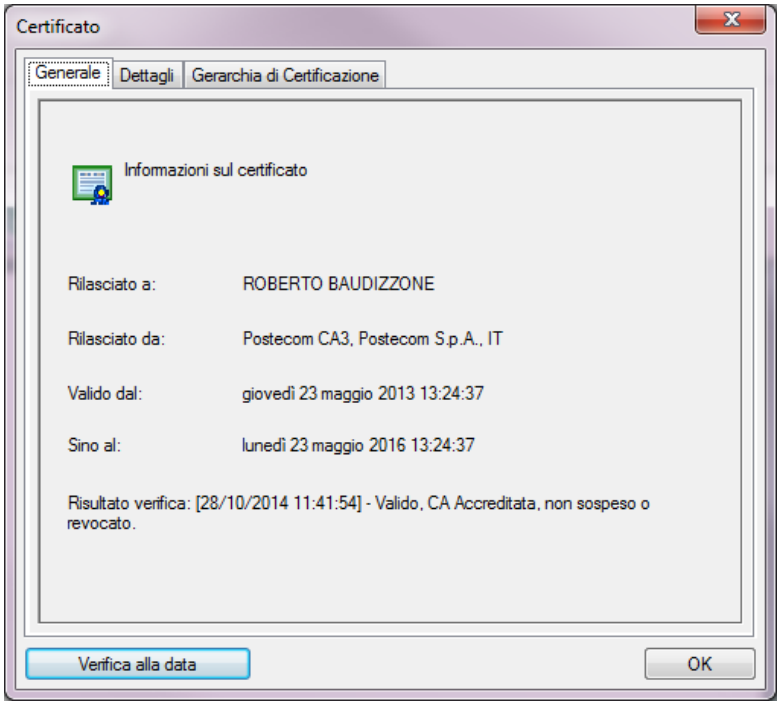
1. la firma è generata con la chiave privata in possesso esclusivo del sottoscrittore, quindi è univocamente collegata a tale soggetto;
2. permette di identificare il sottoscrittore, perché un ente attendibile (certificatore) emette un certificato che associa la chiave pubblica ad una identità;
3. rivela ogni modifica successiva apportata ai dati, perché in fase di verifica non si avrebbe corrispondenza tra l'impronta calcolata sui dati e quella decifrata dalla firma.

1.1.3 Il certificato di chiave pubblica

Elemento fondamentale di una cosiddetta "infrastruttura di chiave pubblica" è il **certificato**, che corrisponde direttamente ad una coppia di chiavi (privata e pubblica) associate ad un titolare.

Si tratta di un insieme di dati (possiamo pensare ad uno speciale documento o ad un file) contenente alcune informazioni fondamentali:

- numero di serie
- dati anagrafici o identificativi del titolare del certificato stesso
- copia della chiave pubblica della coppia associata al titolare
- data di emissione e data di scadenza del certificato
- indicazione del soggetto che ha emesso il certificato (Certificatore)
- informazioni ausiliarie per definire formato e caratteristiche di utilizzabilità del certificato
- indicazioni che consentono di verificare, tramite un accesso automatico al sistema del certificatore, l'eventuale stato di revoca anticipata della validità del certificato
- firma digitale, calcolata sul contenuto del certificato stesso, generata dal "Certificatore"


Certificato
Generale
Dettagli
Gerarchia di Certificazione
Informazioni sul certificato
Rilasciato a: ROBERTO BAUDIZZONE
Rilasciato da: Postecom CA3, Postecom S.p.A., IT
Valido dal: giovedì 23 maggio 2013 13:24:37
Sino al: lunedì 23 maggio 2016 13:24:37
Risultato verifica: [28/10/2014 11:41:54] - Valido, CA Accreditata, non sospeso o revocato.
Verifica alla data
OK

Il motivo per cui un certificato è sempre generato con una vita a termine, quindi con una data di scadenza predefinita, è collegato alla necessità di non mantenere indefinitamente in uso una coppia di chiavi.
Infatti la chiave privata e la pubblica di una coppia sono legate da una relazione matematica. Anche se non è possibile calcolare direttamente la chiave privata essendo nota la pubblica, è possibile usare la cosiddetta "forza bruta" e provare tutte le combinazione sino a trovare la chiave giusta.
La contromisura è usare chiavi di tale lunghezza che un tale procedimento costi un tempo di elaborazione molto lungo, misurabile in anni, anche usando i più veloci supercomputer esistenti ai giorni nostri. E quindi

postulare una durata massima di una coppia di chiavi – registrata nel certificato – molto minore di questo tempo minimo necessario per trovare una chiave privata.

Da notare che la firma digitale apposta dal Certificatore, coprendo tutti gli altri dati contenuti nel certificato stesso, ne protegge l'integrità – per il fatto che eventuali alterazioni verrebbero rivelate, per definizione, in fase di verifica di questa firma – e l'autenticità – perché la firma del certificatore garantisce, sotto la responsabilità di quest'ultimo e nei limiti preventivamente concordati, della veridicità dei dati contenuti –.

1.1.4 Il Certificatore

Sul piano tecnico il soggetto che emette certificati di chiave pubblica si definisce "Autorità di Certificazione" o "*Certification Authority*" o CA.

Una CA è un organo che genera i certificati con il contenuto predefinito e li firma digitalmente con una propria chiave privata (detta "chiave privata di certificazione").
Naturalmente, come qualunque altro soggetto che emette firme ed è quindi dotato di una chiave privata, la CA deve anche essere dotato di un certificato associato alla relativa coppia di chiavi. Tale certificato si chiama "Certificato di CA".

La domanda scontata è: *"ma chi emette allora il certificato della CA? Chi lo firma?"*
La risposta è, in generale: *"una CA di livello superiore"*

Evidentemente questa iterazione di livelli non può ripetersi all'infinito e, prima o poi, la "catena di certificazione" deve arrivare ad una fine.
Il certificato della CA di livello più alto non viene dunque emesso da alcun organo superiore, ma è emesso dalla stessa CA: si tratta di un certificato *"self-signed"* o "di tipo *root*".
La particolarità è che questi certificati sono firmati con la chiave privata appartenente alla stessa coppia la cui chiave pubblica è contenuta nel certificato.

Tornando a livello di definizioni, la **CA** è normalmente intesa come l'organo tecnico, corrispondente ad una chiave privata ed un **certificato di CA**.
Il soggetto o ente che effettivamente svolge le attività correlate, viene definito "Certification Service Provider" o "Fornitore di Servizi di Certificatore", in breve "**Certificatore**".
Un Certificatore può, in generale, gestire più CA. Di solito questo avviene per emettere certificati di diversa tipologia (Firma Digitale, Autenticazione, Marcatura Temporale, ecc.).

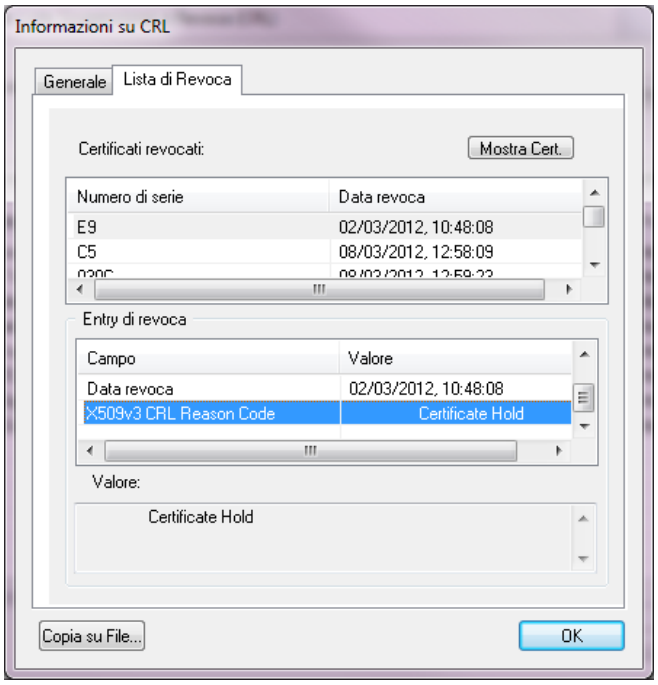
1.1.5 Le liste di Sospensione e Revoca

Come spiegato nella sezione Il certificato di chiave pubblica un certificato nasce con una durata massima prefissata, dipendente dalla scelta commerciale del Certificatore che lo emette, ma comunque determinata dalla lunghezza delle chiavi oggetto di certificazione.

Tuttavia possono verificarsi diverse ragioni per terminare anzitempo la durata di un certificato. Il caso più tipico è quello del legittimo titolare ha perduto – o teme di aver perduto – il possesso esclusivo della chiave privata e vuole evitare che un malintenzionato emetta firme digitali a suo nome. Come si vede si tratta di un'esigenza molto simile al "blocco" di una carta di credito smarrita o rubata.

Ma la revoca di un certificato ha senso soltanto se chi verifica un documento firmato può determinare se il certificato associato alla firma è stato effettivamente revocato.
Lo strumento più comune (e l'unico attualmente fornito obbligatoriamente dai Certificatori) per soddisfa questa esigenza è la Lista di Sospensione e Revoca, o *Certificate Revocation List* (CRL).

Una CRL, banalmente, è una lista di numeri di serie di certificati emessi da una data CA, associati a data, ora e motivo della revoca.



La lista stessa è corredata da un'indicazione di data ed ora di emissione, nonché data ed ora della prossima emissione programmata. La lista è ovviamente firmata digitalmente dalla stessa CA e resa accessibile su un server, ad un indirizzo ben determinato.

Ogni certificato contiene l'indicazione dell'indirizzo Internet a cui è reperibile una copia della CRL. Poiché sia il certificato che la CRL sono firmate digitalmente dalla CA, l'integrità del sistema è molto protetta.
Naturalmente l'uso di queste liste dovrebbe essere automatico in fase di verifica di qualunque firma o certificato, rivelando se il certificato compare nella lista di revoca.

Il Certificatore dovrebbe aggiornare molto frequentemente le proprie CRL, in modo da rendere subito disponibili le revoche che possono avvenire in qualsiasi momento.

NOTA: le CRL si definiscono "Liste di Sospensione e Revoca" perché riportano sia lo stato di revoca che quello di sospensione. Senza entrare troppo nei dettagli possiamo dire che un certificato, di solito, viene posto in uno stato di sospensione (per esempio quando il titolare dichiara telefonicamente di aver perduto il possesso della chiave privata). In seguito, dopo una procedura amministrativa di controllo, la sospensione diventa una revoca a tutti gli effetti, oppure il certificato può sparire dalla lista (per esempio se il titolare dichiara poi di aver ritrovato una smartcard o se la segnalazione telefonica risulta poi non vera).

1.1.6 Il processo di verifica di una firma digitale

La *meccanica* della verifica di una firma consiste nella decifratura della firma stessa mediante la chiave pubblica dell'asserito sottoscrittore – ottenendo una copia dell'impronta – e nel confronto di tale valore con l'impronta calcolata direttamente sui dati, mediante l'appropriata funzione *hash*..

Tuttavia, al di là di verificare che il documento sia integro – operazione matematica priva di criticità – in un contesto reale è importante soprattutto verificare che il sottoscrittore sia veramente chi dice di essere e che il suo certificato sia in corso di validità.

Un documento firmato elettronicamente contiene una copia del certificato di ogni sottoscrittore.
Quindi il sistema di verifica ha a portata di mano la chiave pubblica per eseguire la verifica di integrità sopra descritta.

Ma per verificare l'identità del sottoscrittore il sistema deve verificare se il certificato è autentico.
A tale scopo si deve verificare la firma digitale della CA, apposta al certificato stesso.
Per verificare questa firma occorre disporre del certificato della CA; questo di regola è possibile conservando, a disposizione del proprio sistema, una lista dei certificati delle CA di proprio interesse.

Nel caso in cui il certificato della CA sia stato emesso da un'altra CA di livello superiore occorre risalire tutta la "catena di certificazione" fino al livello più alto (cioè fino a quando si trova il certificato *self-signed*, si veda Il Certificatore).
Giunti a questo punto, per essere sicuri che questo certificato sia autentico, occorre contare su una copia locale veramente attendibile. Se un malintenzionato è in grado di farci considerare attendibile un certificato *self-signed*, può anche costruire facilmente una falsa catena di certificazione e simulare qualunque identità.

In un vero contesto di gestione di documenti informatici questo è il punto più delicato: l'attendibilità dei certificati delle CA. Vedremo come DigitalSign implementa per questo fine accorgimenti ad elevato livello di sicurezza (non tutti i prodotti di firma digitale sul mercato possono dichiarare altrettanto), ma in questa sede ci limitiamo a portare il problema all'attenzione del lettore.

Dicevamo che oltre all'autenticità del certificato (ossia che sia stato veramente emesso da una CA considerata attendibile) occorre anche verificare che il certificato stesso sia in corso di validità.
Una prima verifica, banale, viene eseguita confrontando la data odierna con le date di emissione e scadenza registrate nel certificato stesso.

Quindi occorre verificare se il numero di serie del certificato compaia nella lista di revoca aggiornata pubblicata dal certificatore. Allora il procedimento consiste nei seguenti passi:

1. estrazione, dal certificato, dell'indirizzo da cui scaricare la CRL (CRL Distribution Pount)
2. scaricamento della CRL da tale indirizzo
3. verifica della firma della CA apposta alla CRL
4. verifica che la data ed ora attuali ricadano nell'intervallo tra la data ed ora di emissione e la data ed ora di prossimo aggiornamento pianificato della CRL
5. ricerca del numero di serie del certificato da verificare nella lista contenuta nella CRL

Naturalmente se la lista contiene effettivamente il numero di serie del certificato che stiamo verificando si deve concludere che il certificato, in questo momento, non è valido. E quindi nemmeno il documento che contiene una firma apposta mediante quel certificato, a meno che non sia possibile dimostrare che il documento era stato firmato in precedenza, anteriormente alla revoca.

1.1.7 Le Marche Temporali (*Timestamp*)

Una marca temporale è un documento informatico molto particolare.
È firmato digitalmente da un soggetto definito "Fornitore di Servizi di Marcatura Temporale" (*Timestamp Provider*, TSP) e contiene l'informazione precisa della data ed ora di emissione, nonché il valore di un'impronta fornito dall'utente.

Un utente utilizza questo servizio quando desidera associare una data certa all'esistenza di un documento oppure di una specifica firma apposta al documento:

1. si calcola il valore dell'impronta (*hash*) del documento (o della firma) oggetto della marcatura temporale
2. si trasmette, via Internet, al server del TSP una richiesta contenente l'impronta calcolata
3. si riceve la marca temporale (*timestamp*) dal server del TSP
4. si associa la marca temporale al documento (o alla firma)

Poiché la firma digitale contenuta nel *timestamp* è considerata attendibile (se ci si rivolge a TSP accreditati presso AgID ha pieno valore di prova), sarà possibile dimostrare l'esistenza di un documento (o di una specifica firma), per esempio, in un istante di tempo in cui il certificato del firmatario era sicuramente valido (non scaduto, non revocato).

La procedura di associare ad un documento firmato digitalmente una marca temporale viene anche denominata **consolidamento del valore probatorio**.

1.1.8 I formati di rappresentazione dei documenti firmati

Sin dal 1999, anno di entrata in vigore delle prime regole tecniche in materia di documenti informatici, il formato standard per la rappresentazione dei documenti è stato il PKCS#7: per molti anni questo è stato l'unico formato ritenuto valido.

Un documento PKCS#7 consiste di una “busta crittografica”, ossia una struttura di dati che contiene al proprio interno sia il documento oggetto della firma, sia la firma o le firme digitali, certificati, ecc.

Negli anni più recenti si sono affacciati alla ribalta due altri formati, che nelle ultime evoluzioni della normativa (Deliberazione CNIPA 45/2009) hanno trovato piena dignità:

- il formato PAdES, ossia il PDF corredato di firme digitali e marche temporali al proprio interno
- il formato XAdES, ossia un formato XML che contiene – direttamente nella struttura XML stessa – anche firme e marche temporali

Lo stesso formato PKCS#7 si è arricchito di qualche attributo e viene ora denominato CAdES.

Naturalmente ***DigitalSign***, che ha sempre gestito il formato PKCS#7, supporta pienamente lo standard CAdES, come definito e circoscritto negli accordi di interoperabilità svolti sotto l’egida di DigitPA, nonché lo standard PAdES.

2 Installazione e registrazione

2.1 La procedura di installazione

L'installazione di ***DigitalSign*** è di per sé un processo piuttosto semplice.
Tuttavia va tenuto presente che il prodotto ***DigitalSign*** esiste in diverse edizioni, dai contenuti anche molto differenti tra un'edizione e l'altra.
Inoltre spesso ***DigitalSign*** viene distribuito da distributori, rivenditori, organizzazioni che lo integrano nei propri sistemi e provvedono a fornire un ambiente di installazione integrato, spesso congiuntamente a software specifico per particolari smartcard, lettori, ecc.; in tal caso occorre seguire le istruzioni pratiche del fornitore.

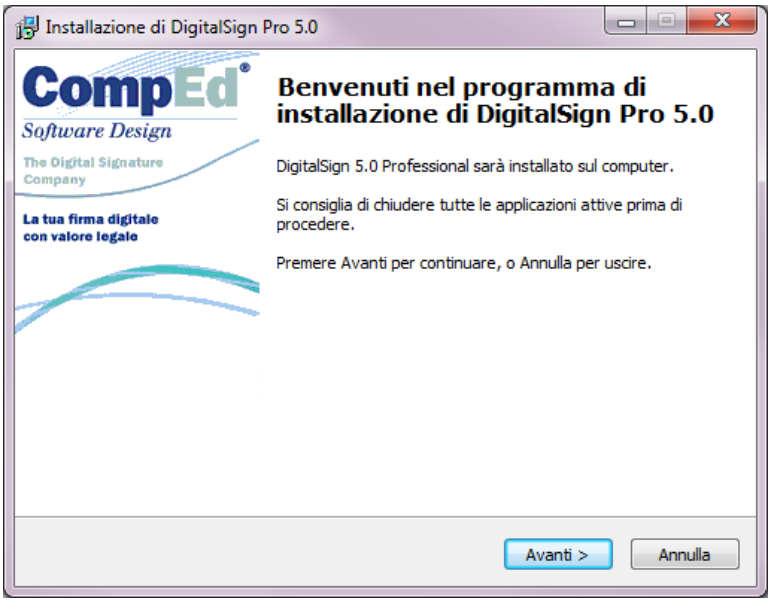
In generale l'installazione di ***DigitalSign*** consiste in un solo file eseguibile da lanciare per avviare il processo di installazione vero e proprio.

Ad esempio, scaricando DigitalSign Professional da un sito Internet si può ottenere il file

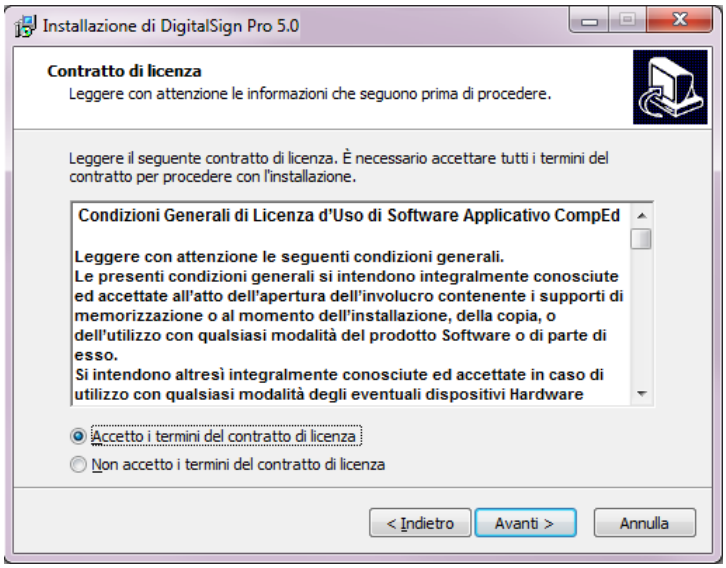
`DS50_PRO_R06.EXE`

Questo sarebbe il file di installazione per DigitalSign Professional 5.0.3.6.

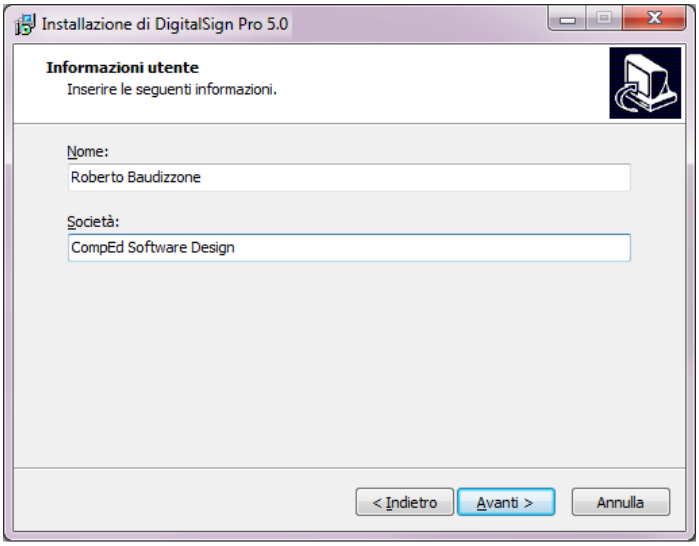
Normalmente l'utente che vede questo file attraverso gli strumenti del proprio sistema farà doppio click su questo programma per avviare il processo di installazione.


Installazione di DigitalSign Pro 5.0
CompEd
Software Design
The Digital Signature Company
La tua firma digitale con valore legale
Benvenuti nel programma di installazione di DigitalSign Pro 5.0
DigitalSign 5.0 Professional sarà installato sul computer.
Si consiglia di chiudere tutte le applicazioni attive prima di procedere.
Premere Avanti per continuare, o Annulla per uscire.
Avanti >
Annulla

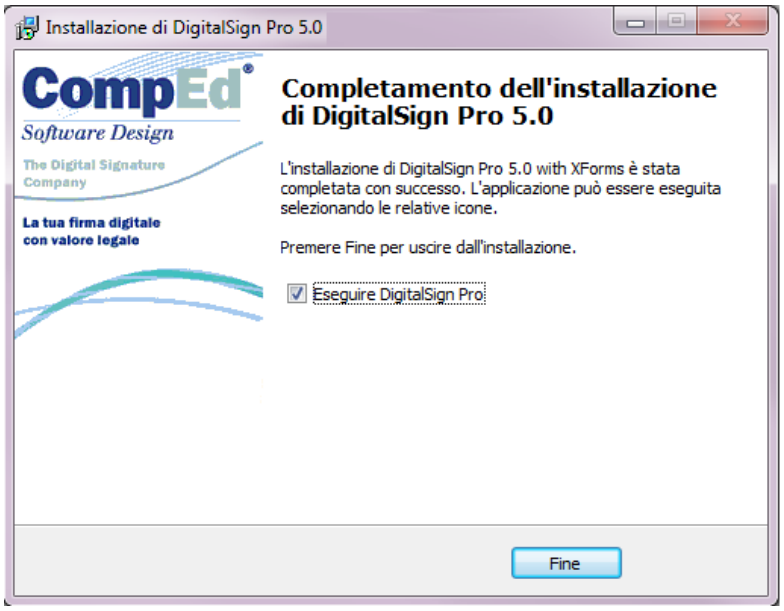
Procedendo fase dopo fase, agendo sul bottone **Avanti**, si dovrà innanzitutto accettare le condizioni di licenza d'uso:


Installazione di DigitalSign Pro 5.0
Contratto di licenza
Leggere con attenzione le informazioni che seguono prima di procedere.
Leggere il seguente contratto di licenza. È necessario accettare tutti i termini del contratto per procedere con l'installazione.
Condizioni Generali di Licenza d'Uso di Software Applicativo CompEd
Leggere con attenzione le seguenti condizioni generali.
Le presenti condizioni generali si intendono integralmente conosciute ed accettate all'atto dell'apertura dell'involucro contenente i supporti di memorizzazione o al momento dell'installazione, della copia, o dell'utilizzo con qualsiasi modalità del prodotto Software o di parte di esso.
Si intendono altresì integralmente conosciute ed accettate in caso di utilizzo con qualsiasi modalità degli eventuali dispositivi Hardware
Accetto i termini del contratto di licenza
Non accetto i termini del contratto di licenza
< Indietro
Avanti >
Annulla

Quindi introdurre il proprio nominativo e quello dell'organizzazione di appartenenza, notando che questi dati non vengono trasmessi da DigitalSign, ma vengono solo registrati nel sistema.
È appena il caso di notare che prima di installare ed utilizzare una copia di ***DigitalSign*** occorre averne acquistato regolare licenza.



In generale l'utente accetterà le proposte di default presentate dal programma di installazione (percorso, moduli da installare, cartella del menu Start), sino al completamento dell'installazione (che talvolta, se non avevamo chiusi tutte le applicazioni prima di iniziare l'installazione, può richiedere il riavvio del sistema).


Installazione di DigitalSign Pro 5.0
CompEd
Software Design
The Digital Signature Company
La tua firma digitale con valore legale
Completamento dell'installazione di DigitalSign Pro 5.0
L'installazione di DigitalSign Pro 5.0 with XForms è stata completata con successo. L'applicazione può essere eseguita selezionando le relative icone.
Premere Fine per uscire dall'installazione.
Eseguire DigitalSign Pro
Fine

Si rammenta che l'installazione di DigitalSign NON COMPRENDE l'installazione di software specifico per lettori e/o smartcard e che tale software deve essere installato separatamente.

2.1.1 L'installazione "silente"

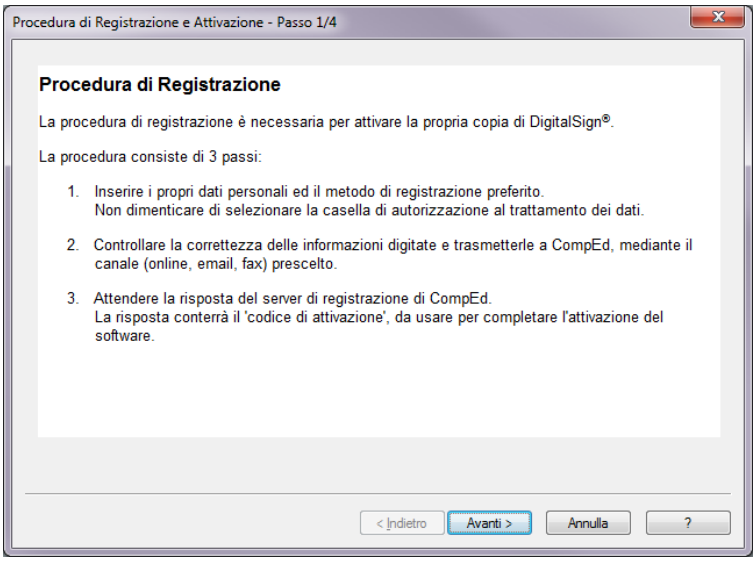
Alcune edizioni di ***DigitalSign***, soprattutto quelle distribuite da grandi organizzazioni, supportano una modalità di esecuzione silente: il processo di installazione viene eseguito con le impostazioni predefinite, senza richiedere l'intervento dell'operatore.

Nei casi in cui questa modalità è supportata può venire attivata a livello di linea comandi. Ad esempio, se il file di installazione fosse **`DS50_PRO_R06.exe`**, la linea comandi può essere:

- **`DS50_PRO_R06 /silent`**
  In questo caso il processo di installazione mostra soltanto la schermata con il progresso dell'installazione e null'altro, senza fermarsi a chiedere conferme o scelte dell'operatore.
- **`DS50_PRO_R06 /verysilent`**
  In questo caso il processo di installazione non mostra nulla e l'installazione avviene in modo invisibile per l'utente.

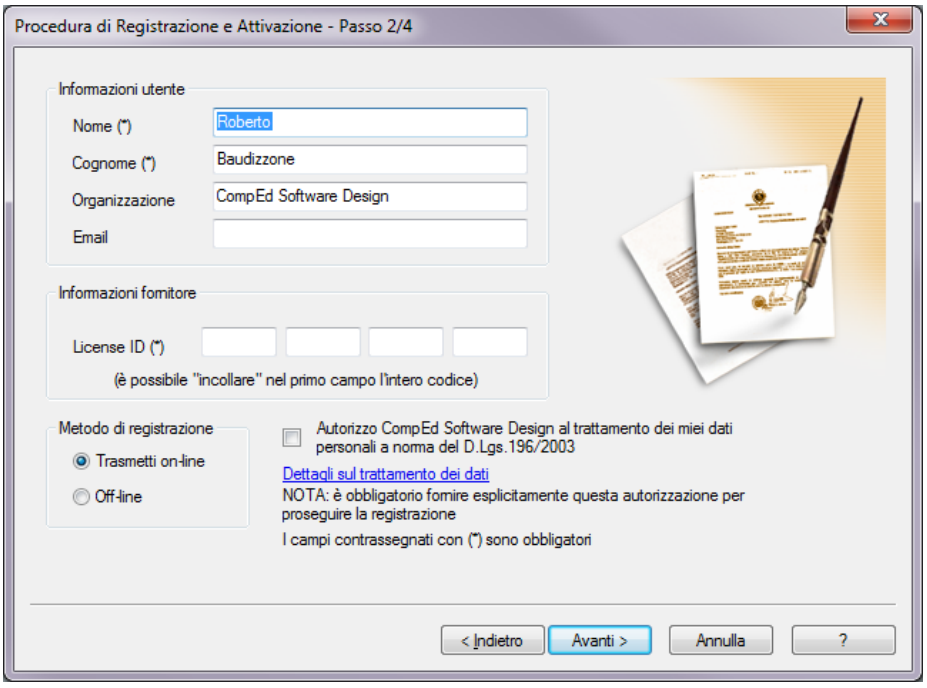
2.2 Registrazione ed Attivazione

DigitalSign prevede l'esecuzione di una procedura di registrazione, che per alcune edizioni richiede l'introduzione di un codice. Al primo avvio la procedura è avviata automaticamente:


Procedura di Registrazione e Attivazione - Passo 1/4
Procedura di Registrazione
La procedura di registrazione è necessaria per attivare la propria copia di DigitalSign®.
La procedura consiste di 3 passi:
1. Inserire i propri dati personali ed il metodo di registrazione preferito.
Non dimenticare di selezionare la casella di autorizzazione al trattamento dei dati.
2. Controllare la correttezza delle informazioni digitate e trasmetterle a CompEd, mediante il canale (online, email, fax) prescelto.
3. Attendere la risposta del server di registrazione di CompEd.
La risposta conterrà il 'codice di attivazione', da usare per completare l'attivazione del software.
< Indietro
Avanti >
Annulla
?

La prima schermata si limita ad informare l'utente sui contenuti della procedura.

Con il bottone **Avanti** si procede:

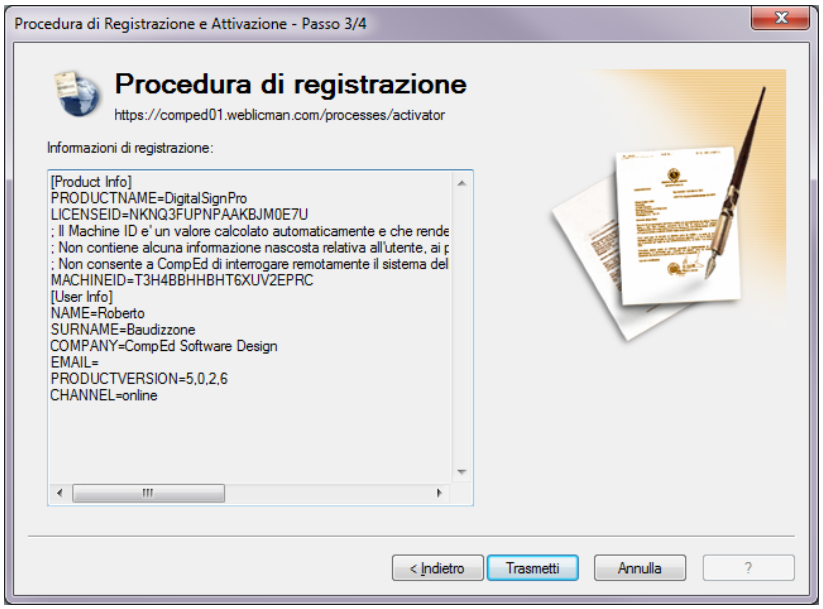


I campi del primo riquadro riguardano i dati personali di registrazione. Tutti i campi contrassegnati con il simbolo '**(*)**' sono obbligatori. L'indirizzo Email è obbligatorio in caso di attivazione Off-line.

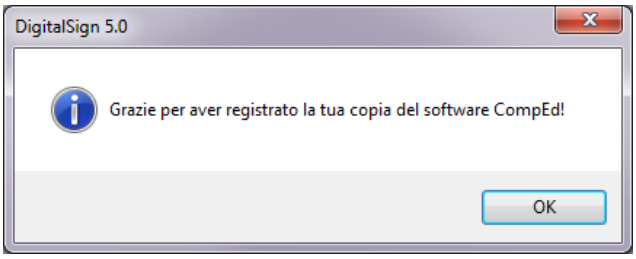
Nel secondo riquadro occorre inserire il Codice Licenza ricevuto dal fornitore, necessario per attivare la propria copia di DigitalSign (si noti che non tutte le edizioni di prodotto richiedono un Codice Licenza, nel qual caso non è mostrato il simbolo di obbligatorietà **(*)**).

Il terzo riquadro, Metodo di registrazione, permette di scegliere la modalità per operare la registrazione/attivazione i dati a CompEd:

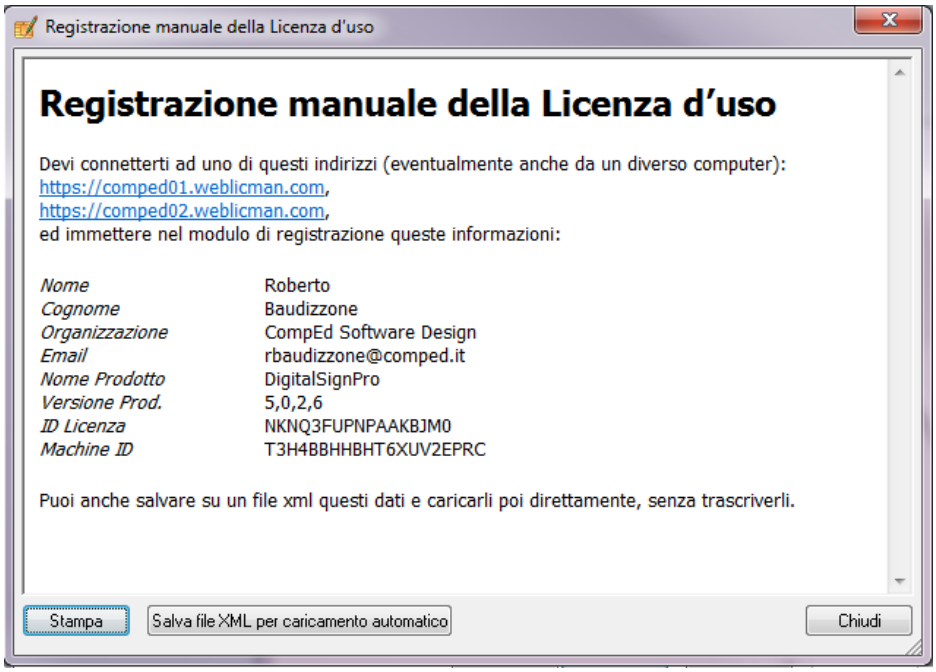
- **Trasmetti on-line** – è il metodo preferito: DigitalSign si connette direttamente al server di CompEd e trasmette via web i dati di registrazione, così che il server possa immediatamente generare e ritrasmettere il codice di attivazione completando l'attivazione in un attimo..
  Naturalmente questo metodo può essere usato solo se il computer ha un collegamento ad Internet privo di restrizioni per l'accesso alla rete.



Come si vede la finestra visualizza il contenuto dei dati trasmessi e l'indirizzo di spedizione (quest'ultimo può essere utile per la diagnostica di eventuali problemi di rete; si noti che diverse versioni del software possono trasmettere a diversi indirizzi, quello riportato in figura ha solo valore indicativo).
Con il bottone **Trasmetti** avviene il collegamento effettivo e l'attivazione si completa in un attimo.



- **Off-Line** – questa modalità dovrebbe essere utilizzata quando il computer su cui si effettua l'installazione non ha modo d connettersi direttamente con il server di registrazione via Internet.
  Al passo successivo il sistema si limita a presentare i dati di registrazione ed attendere il bottone Avanti, dopo di che presenterà questa finestra di dialogo:

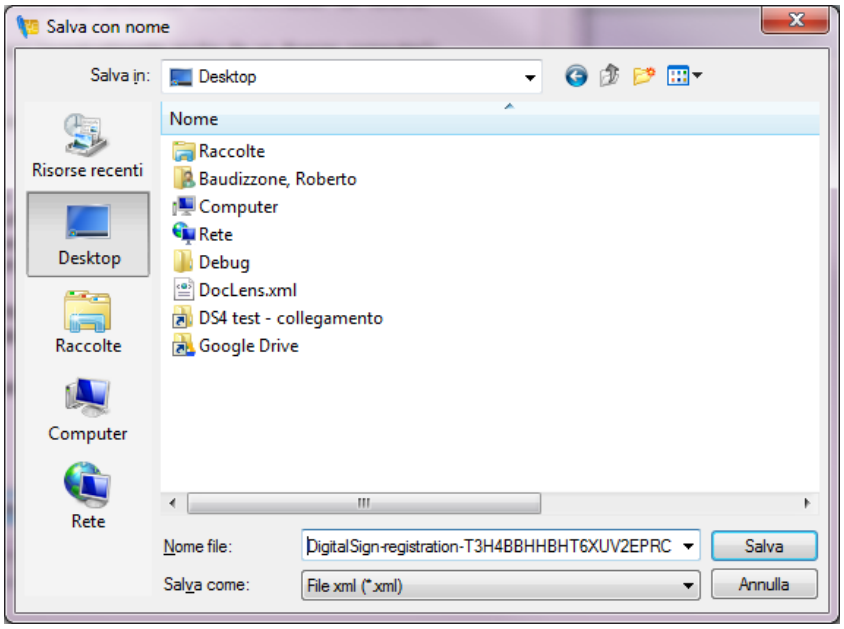

Registrazione manuale della Licenza d'uso
Registrazione manuale della Licenza d'uso
Devi connetterti ad uno di questi indirizzi (eventualmente anche da un diverso computer):
https://comped01.weblicman.com,
https://comped02.weblicman.com,
ed immettere nel modulo di registrazione queste informazioni:
Nome Roberto
Cognome Baudizzone
Organizzazione CompEd Software Design
Email rbaudizzone@comped.it
Nome Prodotto DigitalSignPro
Versione Prod. 5,0,2,6
ID Licenza NKNQ3FUPNPAAKBJM0
Machine ID T3H4BBHHBHT6XUV2EPRC
Puoi anche salvare su un file xml questi dati e caricarli poi direttamente, senza trascriverli.
Stampa
Salva file XML per caricamento automatico
Chiudi

Nelle prossime sezioni illustriamo le diverse modalità per completare questa procedura off-line

2.2.1 Registrazione off-line: modalità XML

Questa modalità è la più comoda, perché non richiede di digitare nulla, ma si basa sul passaggio di un file di parametri.

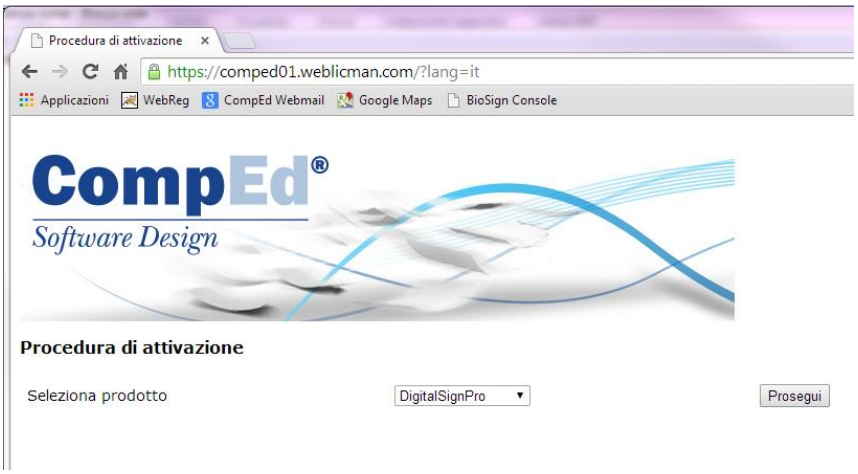
Dalla schermata mostrata in fondo alla sezione precedente si usi il bottone Salva file XML per caricamento automatico. Il sistema chiede di indicare una posizione per salvare il file, per esempio sceglieremo il Desktop:



Il file ha un nome piuttosto lungo, composto dal prefisso **DigitalSign-registration-** seguito dal valore del Machine ID e dall'estensione **.xml** (può essere utile ai rivenditori che possono così classificare diversi file relativi a diverse installazioni). Premiamo il bottone **Salva**.

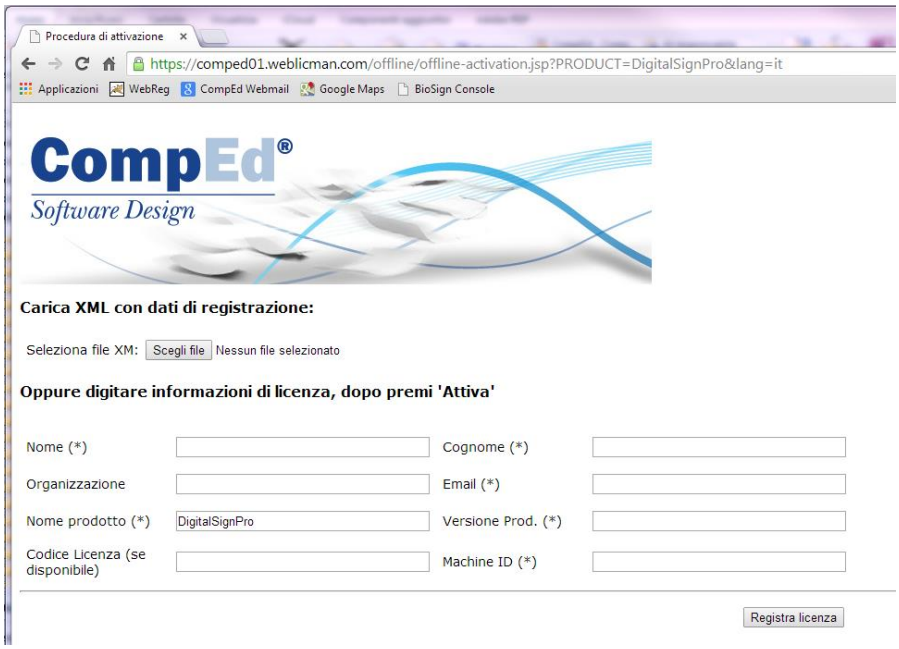
Come indicato dalla schermata della pagina precedente dobbiamo ora aprire un browser Internet (verosimilmente da un diverso computer con accesso a Internet, altrimenti avremmo potuto usare la registrazione Online) e accedere all'indirizzo https://comped01.weblicman.com

Vedremo una pagina di questo tipo:



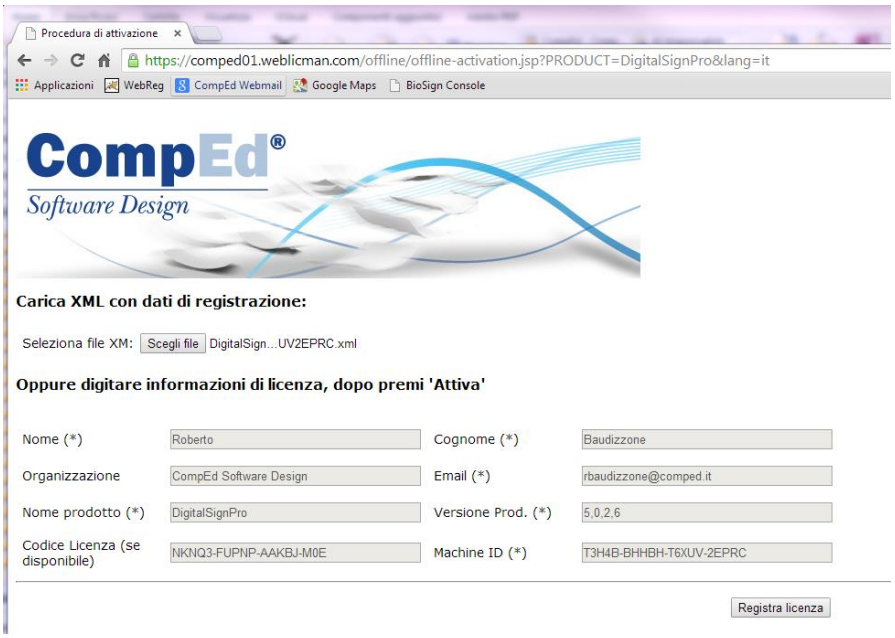
Dopo aver selezionato il prodotto corrispondente alla propria esigenza si agisce su **Prosegui**.

La prossima schermata (ancora in comune con il caso di registrazione manuale) si presenta così:

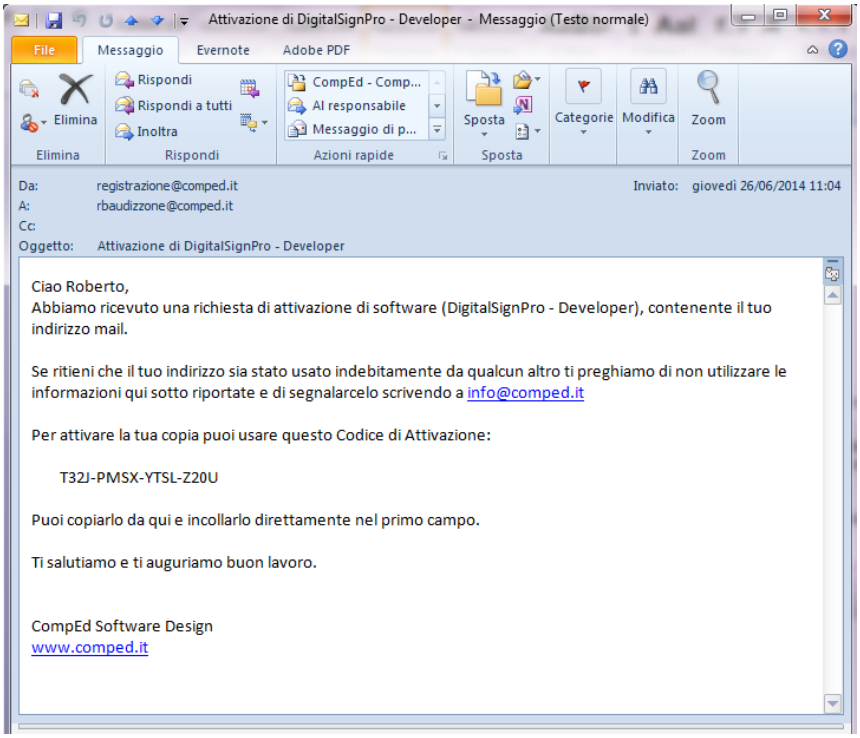


Qui useremo il bottone Scegli File, puntando al file XML salvato nel passo precedente. Evidentemente, se ci troviamo su un diverso computer, dovremo aver messo a disposizione il file mediante una chiavetta USB, una email, una cartella condivisa.

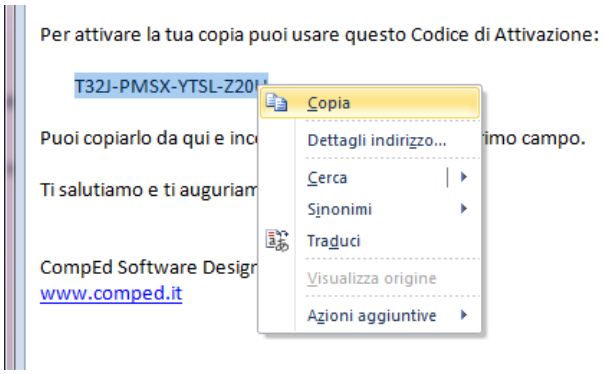
Appena selezionato il file vedremo i campi della registrazione riempirsi automaticamente con il contenuto del file XML:



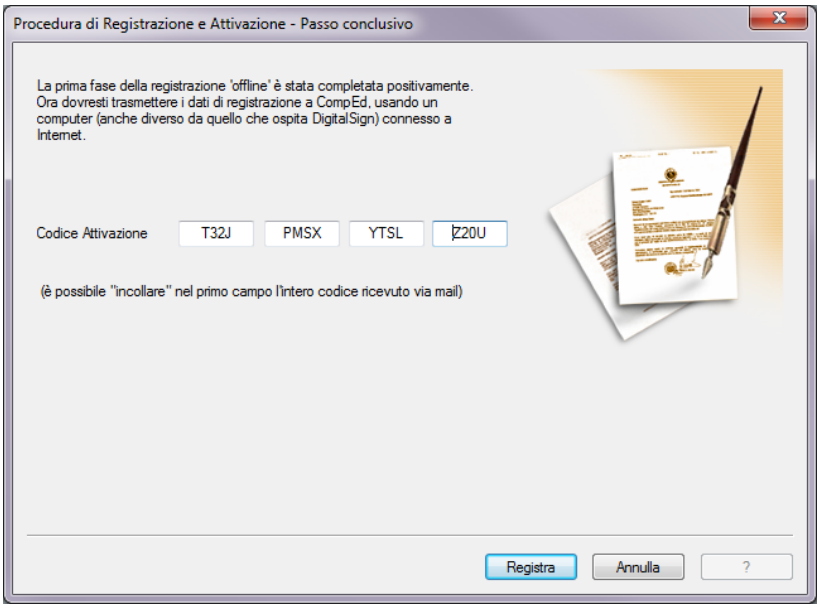
Agendo sul bottone Registra Licenza il sistema genera il Codice di Attivazione e lo trasmette via mail all'indirizzo specificato.


Attivazione di DigitalSignPro - Developer - Messaggio (Testo normale)
File
Messaggio
Evernote
Adobe PDF
Elimina
Rispondi
Rispondi a tutti
Inoltra
CompEd - Comp...
Al responsabile
Messaggio di p...
Sposta
Categorie
Modifica
Zoom
Da: registrazione@comped.it
A: rbaudizzone@comped.it
Cc:
Oggetto: Attivazione di DigitalSignPro - Developer
Inviato: giovedì 26/06/2014 11:04
Ciao Roberto,
Abbiamo ricevuto una richiesta di attivazione di software (DigitalSignPro - Developer), contenente il tuo indirizzo mail.
Se ritieni che il tuo indirizzo sia stato usato indebitamente da qualcun altro ti preghiamo di non utilizzare le informazioni qui sotto riportate e di segnalarcelo scrivendo a info@comped.it
Per attivare la tua copia puoi usare questo Codice di Attivazione:
T32J-PMSX-YTSL-Z20U
Puoi copiarlo da qui e incollarlo direttamente nel primo campo.
Ti salutiamo e ti auguriamo buon lavoro.
CompEd Software Design
www.comped.it

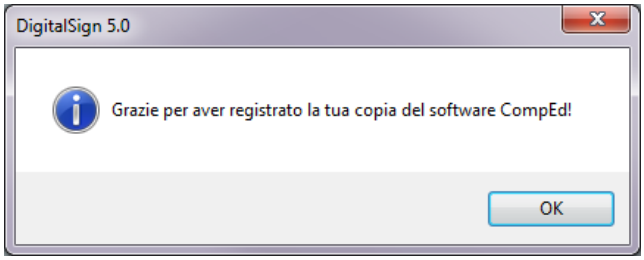
A questo punto selezioneremo e copieremo il Codice di Attivazione dal testo della mail:



E lo incolleremo direttamente nella finestra di dialogo di DigitalSign che appare dopo aver premuto **Chiudi** in quella di Registrazione Manuale:


Procedura di Registrazione e Attivazione - Passo conclusivo
La prima fase della registrazione 'offline' è stata completata positivamente.
Ora dovresti trasmettere i dati di registrazione a CompEd, usando un computer (anche diverso da quello che ospita DigitalSign) connesso a Internet.
Codice Attivazione
T32J
PMSX
YTSL
Z20U
(è possibile "incollare" nel primo campo l'intero codice ricevuto via mail)
Registra
Annulla
?

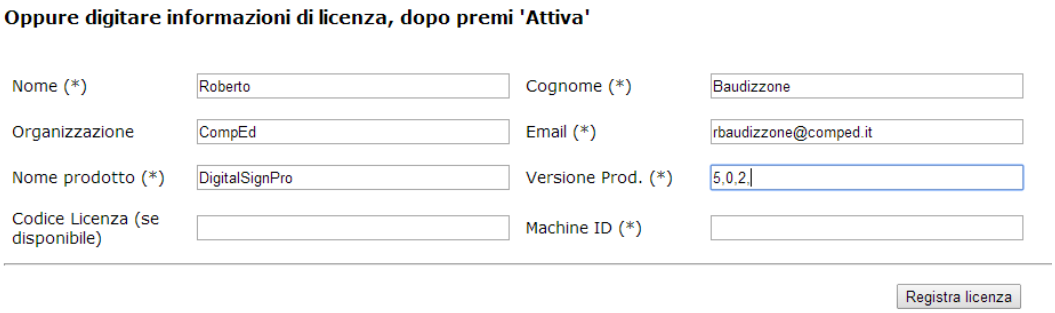
Con **Registra** il processo si conclude:



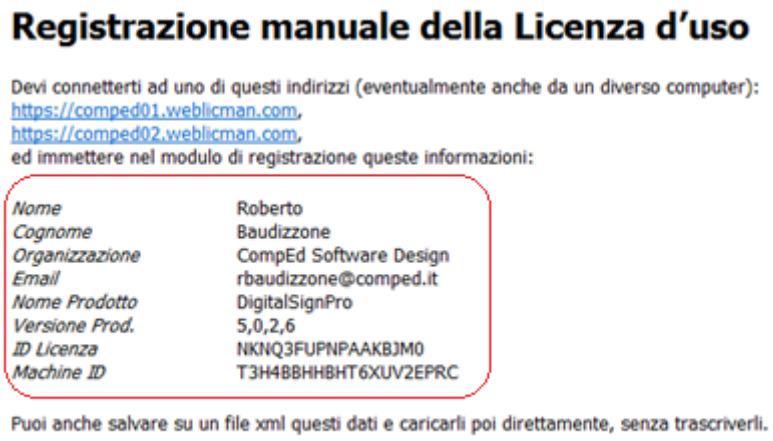
2.2.2 Registrazione off-line: modalità manuale

Questa procedura è quasi identica a quella illustrata al passo precedente.

La differenza consiste nel fatto che non si utilizza il file XML di passaggio dei dati, ma occorre digitare manualmente i dati nella form…



… leggendoli dalla schermata di registrazione manuale:

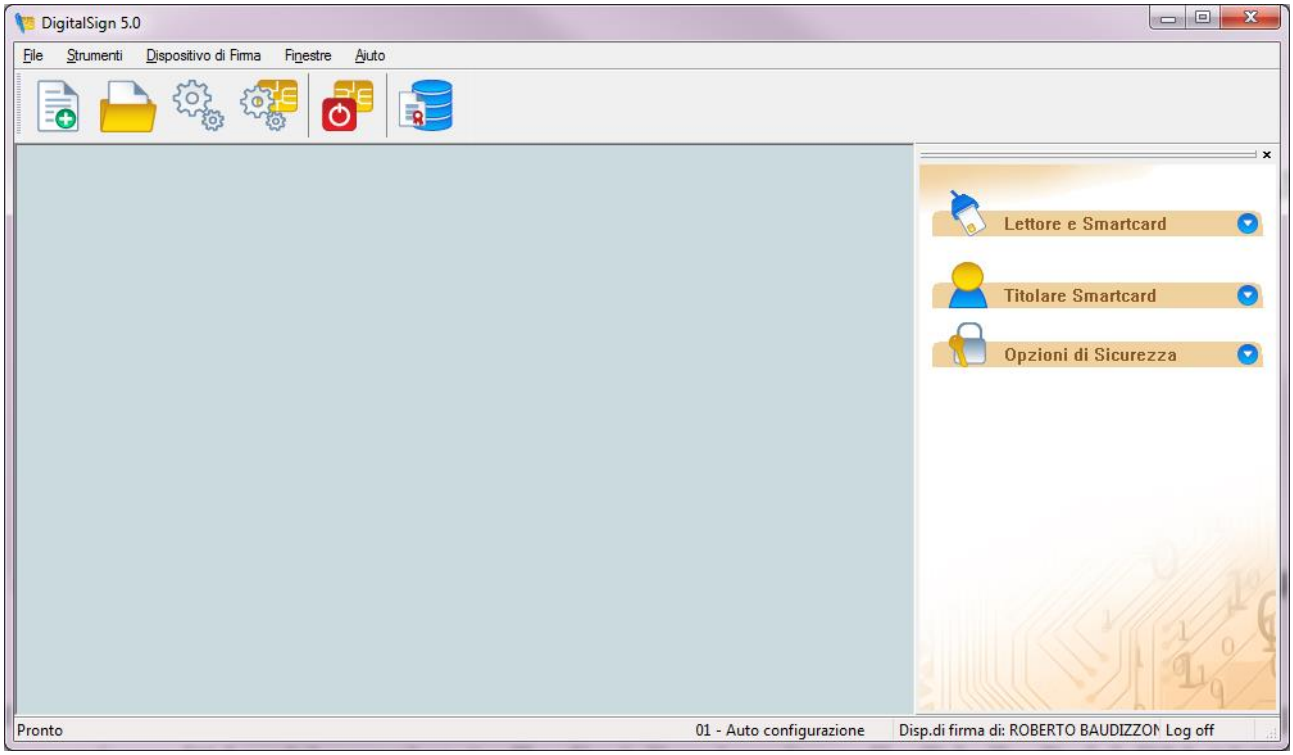

Registrazione manuale della Licenza d'uso
Devi connetterti ad uno di questi indirizzi (eventualmente anche da un diverso computer):
https://comped01.weblicman.com,
https://comped02.weblicman.com,
ed immettere nel modulo di registrazione queste informazioni:
Nome Roberto
Cognome Baudizzone
Organizzazione CompEd Software Design
Email rbaudizzone@comped.it
Nome Prodotto DigitalSignPro
Versione Prod. 5,0,2,6
ID Licenza NKNQ3FUPNPAAKBJM0
Machine ID T3H4BBHHBHT6XUV2EPRC
Puoi anche salvare su un file xml questi dati e caricarli poi direttamente, senza trascriverli.

Per il resto la procedura è identica a quella precedente.

3 Riferimento

3.1 DigitalSign sullo schermo

3.1.1 La finestra principale



La finestra principale di ***DigitalSign*** presenta un menu di opzioni di base ed una vista sui pannelli informativi.

In realtà capita di rado di vedere la finestra principale priva di altre finestre, perché normalmente l'applicazione si apre direttamente mostrando una finestra documento.

Da notare che la zona grigia della finestra principale è un'area *drag & drop*, ossia supporta il trascinamento degli oggetti. Questo significa che se da un'altra applicazione (tipicamente Explorer/Gestione Risorse) si trascina un documento in quest'area, il documento viene immediatamente aperto da DigitalSign.

In ogni caso La finestra principale di DigitalSign presenta alcuni elementi fondamentali:

- Una barra menu

- Una barra strumenti

- Un'area di pannelli informativi

- Una barra di stato

3.1.2 La finestra documento

DigitalSign gestisce i documento all'interno di una di queste finestre, realizzando una vera e propria modalità **WYSIWYS** *(What You See Is What You Sign)*.

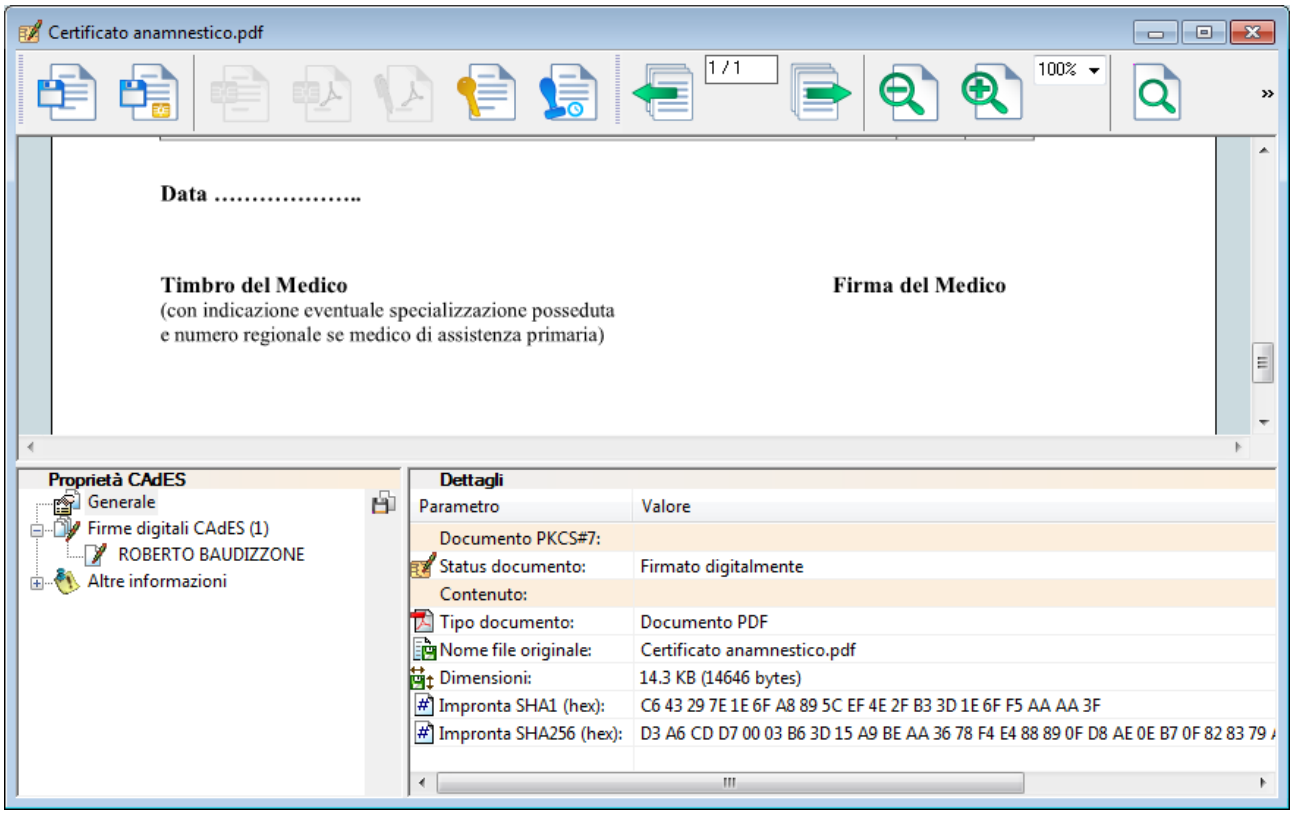
Nelle prossime due sezioni illustriamo questi due tipi di documento (CAdES e PAdES), ma in ogni caso la finestra documento è composta da diverse aree:

- una **toolbar documento**, diversa da quella della finestra principale, ma che opera con lo stesso principio (ogni icona è associata ad una diversa funzione di menu);
- un'area **Viewer**, nella quale viene presentato all'utente il contenuto del documento su cui si sta operando;
- un'area Proprietà, nella quale sono presentati gli oggetti contenuti nella struttura del documento (firme, certificati, ecc.);
- un'area Dettagli, in cui sono visualizzate le informazioni di dettaglio riguardanti l'oggetto correntemente selezionato nell'area "Proprietà"

3.1.2.1 Documenti di tipo CAdES

Sono i documenti che ***DigitalSign*** ha sempre gestito, anche nelle vecchie versioni.
Quando si intende produrre un documenti di questo tipo partendo da un documento di qualunque tipo si costruisce una struttura di dati standard che include al proprio interno sia il documento originale – bit per bit, senza modifiche – che tutti gli elementi utili per i nostri scopi: la firma o le firme digitali, il certificato o i certificati associati alla firma, eventuali marche temporali o altri attributi, eventuali altri oggetti a supporto della crittografia, ecc.

DigitalSign riproduce visualmente una struttura del genere:



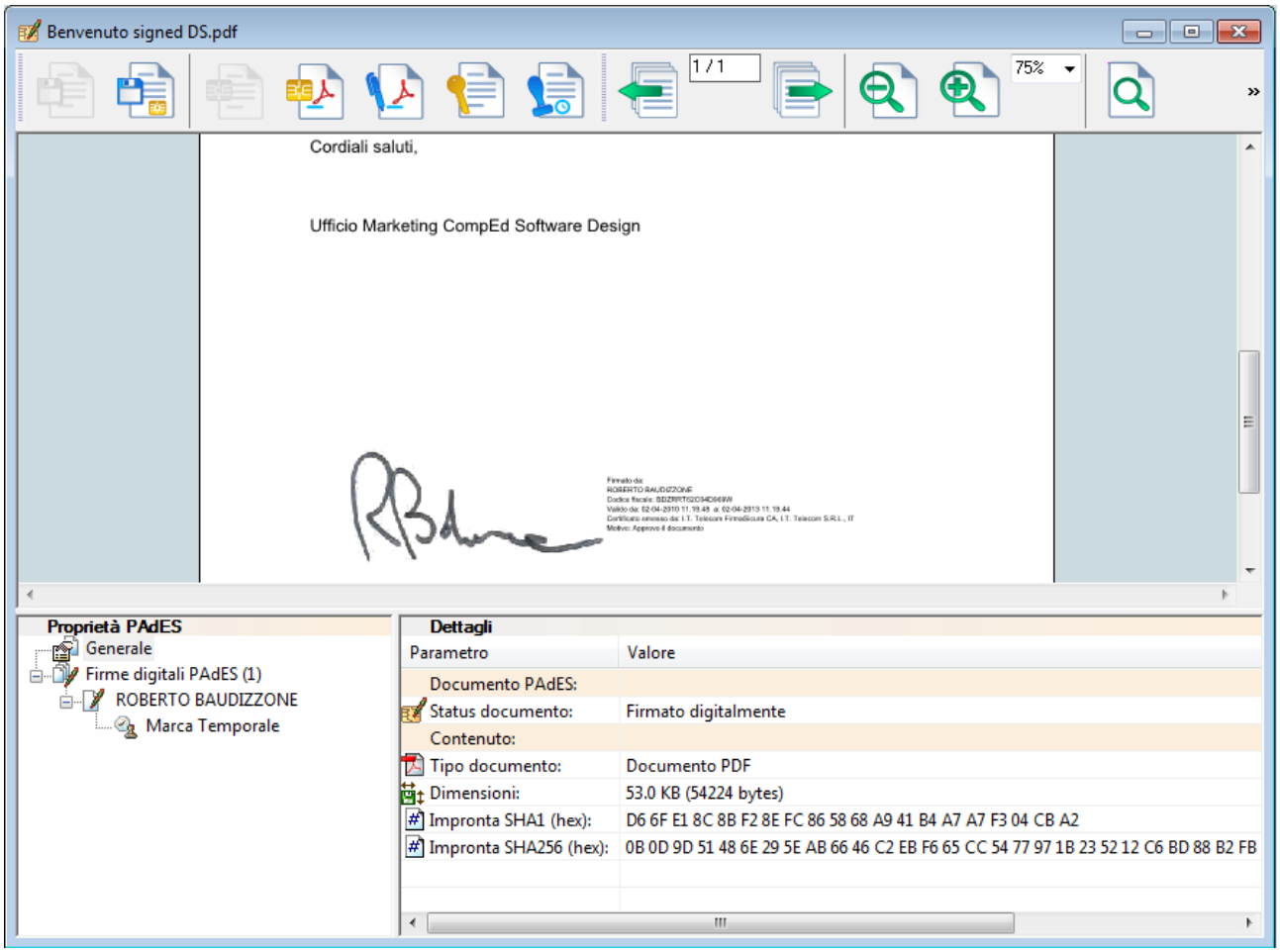
La parte del viewer rappresenta il documento originale (di tipo PDF in questo caso), mentre il pannello in basso a sinistra [**Proprietà CAdES**] consente di esaminare tutti gli elementi del documento e quello in basso a destra espande i dettagli dell'elemento correntemente selezionato nel pannello delle proprietà.

3.1.2.2 Documenti di tipo PAdES

I documenti PDF possono essere corredati di firme digitali e marche temporali direttamente al proprio interno, senza ricorrere alla sovrastruttura della busta crittografica.
Tecnicamente, per ogni firma apposta al documento:

- si aggiunge in coda al file uno spazio vuoto destinato ad accogliere i dati effettivi della firma digitale;
- si aggiunge, in coda allo spazio della firma, una appendice che conterrà le direttive di presentazione grafica della firma (un eventuale oggetto grafico, elementi testuali, posizione, dimensioni, ..);
- si calcola la firma digitale sul complesso del documento originario concatenato con l'appendice di presentazione della firma
- si inserisce la firma così calcolata nello spazio vuoto riservato allo scopo

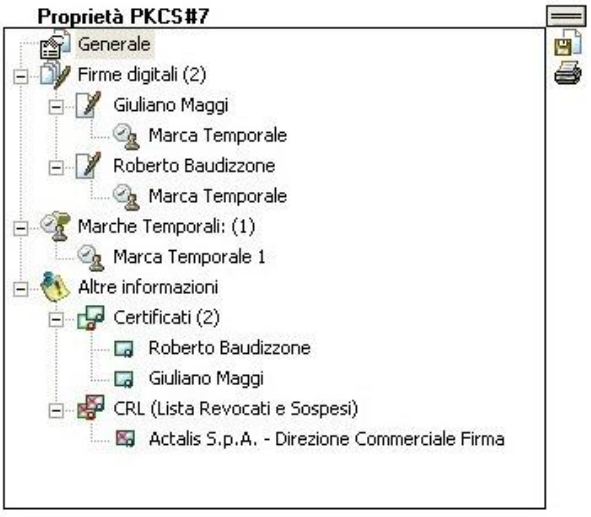
DigitalSign usa per presentare questi documenti lo stesso stile visto prima:



Il vantaggio "ergonomico" del formato PAdES consiste proprio nella possibilità di includere nella presentazione del documento anche una immagine che emula la firma autografa, solitamente apprezzato dagli utenti dei documenti così firmati.

3.1.2.3 Finestra documento: area "Proprietà"

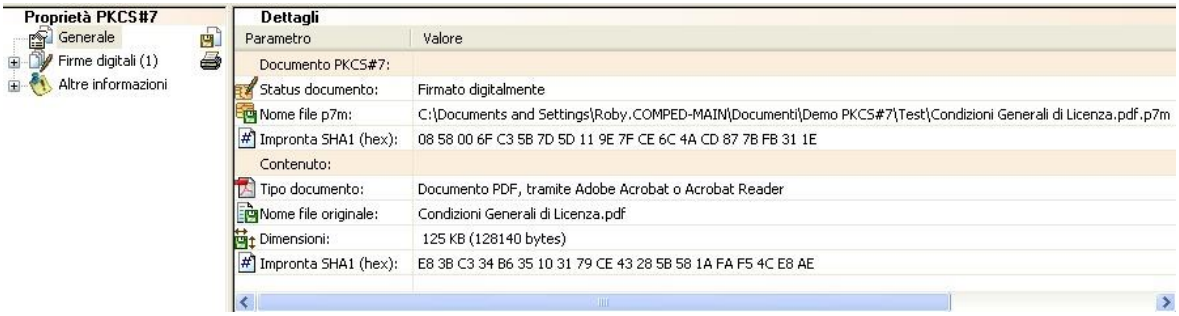
Questo riquadro, visualizzato in basso a sinistra nella finestra documento, rappresenta l'insieme degli elementi di informazione che, oltre al documento elettronico, sono contenuti nel file PKCS#7 che rappresenta il documento informatico aperto.



La visualizzazione è presentata come un albero il cui elemento principale è un riepilogo generale. Per gli elementi in cui è riportato il simbolo '+' è possibile agire con il mouse sul simbolo al fine di aprire la visualizzazione del sottoalbero. Analogamente, se è mostrato un simbolo '-', si può richiudere il sottoalbero agendo sul simbolo.

I rami principali dell'albero possono essere:

- **Generale**

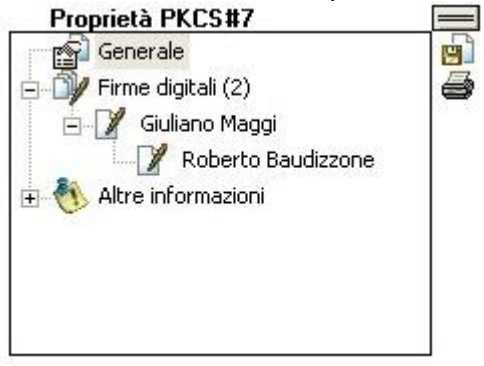

Proprietà PKCS#7
Generale
Firme digitali (1)
Altre informazioni
Dettagli
Parametro
Valore
Documento PKCS#7:
Status documento:
Firmato digitalmente
Nome file p7m:
C:\Documents and Settings\Roby.COMPED-MAIN\Documenti\Demo PKCS#7\Test\Condizioni Generali di Licenza.pdf.p7m
Impronta SHA1 (hex):
08 58 00 6F C3 5B 7D 5D 11 9E 7F CE 6C 4A CD 87 7B FB 31 1E
Contenuto:
Tipo documento:
Documento PDF, tramite Adobe Acrobat o Acrobat Reader
Nome file originale:
Condizioni Generali di Licenza.pdf
Dimensioni:
125 KB (128140 bytes)
Impronta SHA1 (hex):
E8 3B C3 34 B6 35 10 31 79 CE 43 28 5B 58 1A FA F5 4C E8 AE

Questo sottoalbero non può ulteriormente diramarsi e contiene un riepilogo generale del contenuto del documento informatico.
Si tratta dell'unico elemento di un documento PKCS#7 che viene automaticamente compilato al caricamento di un documento non ancora firmato o elaborato in alcun modo.
L'utente può ricavare da questa schermata, tra l'altro, il valore dell'impronta del documento contenuto e, se già salvato sul file, anche l'impronta del documento PKCS#7 complessivo

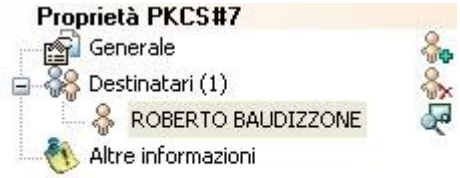
- **Firme digitali**
Questo sottoalbero, se esistente, contiene una o più *foglie*, ciascuna delle quali corrisponde a una firma digitale apposta al documento.
DigitalSign supporta firme multiple apposte ad un documento, secondo due diverse modalità:

  - ***Firme parallele, o congiunte*** (firme apposte allo stesso livello, riferite al documento, senza reciproci riferimenti tra una firma e l'altra)

  - ***Firme gerarchiche, o controfirme*** (apposte a livelli diversi, una controfirma è riferita alla firma di livello superiore e - solo indirettamente – al documento)



- **Destinatari di cifratura**



Questo sottoalbero, se esistente, contiene una o più *foglie*, ciascuna delle quali corrisponde a un destinatario di cifratura associato al documento.
Si ricordi che se questa lista di destinatari è vuota il documento non viene cifrato e rimane in chiaro.
Con l'aggiunta di un primo destinatario alla lista l'autore del messaggio viene automaticamente aggiunto a sua volta, per consentirgli di riaprire il documento.
Ogni destinatario è mostrato da un simbolo seguito dal nominativo del destinatario

- **Marche temporali**

Questo sottoalbero, se esistente, contiene una o più *foglie*, ciascuna delle quali corrisponde a una marca temporale già associata al documento.

- **Altre informazioni**

In questa sezione dell'albero trovano posto, normalmente, i certificati: ad ogni firma è necessariamente associato un certificato, qui è possibile ispezionarne tutti i dettagli.
Opzionalmente è possibile includere nel documento firmato anche una copia della CRL (Lista di Sospensione e Revoca); lo scopo di tale inclusione, seguita dalla marcatura temporale, è di corredare il documento firmato di un set di elementi di prova per attestare che il certificato usato per la firma era valido in un istante di tempo certo.

Il lato destro di questo pannello ospita una *toolbar* verticale attraverso la quale l'utente può accedere rapidamente alle operazioni possibile, senza dover utilizzare il menu o le *toolbar* della finestra principale.
Naturalmente le operazioni possibili variano secondo il tipo di elemento correntemente selezionato.
Passando con il cursore sulle relative icone si ottiene una spiegazione di ogni funzione.

Le stesse funzioni sono anche disponibili tramite un "pop-up" menu che appare agendo con il tasto destro su un elemento della finestra:

3.1.2.4 Finestra documento: area "Dettagli"

Questo riquadro della finestra documento mostra in generale una tabella in due colonne nella quale sono rappresentate le informazioni di dettaglio disponibili per l'oggetto correntemente selezionato nell'area proprietà CAdES.

L'esempio che segue mostra il contenuto completo di questo riquadro quando visualizza i dettagli di una **firma digitale**:

Dettagli	
Parametro	Valore
Risultato verifica:	
Stato della firma:	Valido
Stato del certificato:	[18/06/2014 15:52:10] - Valido, CA Accreditata, non sospeso o revocato.
Certificato:	
Algoritmo certificato:	sha256WithRSAEncryption
S.N. certificato:	61ED
Valido dal:	giovedì 23 maggio 2013 14:24:37
Valido sino al:	lunedì 23 maggio 2016 14:24:37
Soggetto:	
Nome:	ROBERTO
Cognome:	BAUDIZZONE
Codice fiscale:	BDZRRT62C04D969W
Data di nascita:	<non disponibile>
Ruolo:	<non disponibile>
Organization:	COMPED PROGETTI SRL/01743900993
Organization Unit:	<non disponibile>
qcStatements:	1. Questo è un Certificato Qualificato conforme agli Annex I e II della Direttiva EU 1999/93/CE 2. Questo certificato riporta un periodo di "retention" da
Paese:	IT
Certificato emesso da:	
Nome:	Postecom CA3, Postecom S.p.A., IT
Paese:	IT
Firma documento:	
Algoritmo di firma:	RSA-sha256 (1024)
Firma digitale (hex):	175B 5D6A 485E 6873 5D81 55C8 372B 54F8 5958 0F6C 1233 7491 AF09 9F8C B01C B339 C236 1B4B 3D88 D62D 581D 7FD7 6B3F 21AB 758A 85FF 8F83 5A1
Attributi 'signed':	
contentType	pkcs7-data
signingTime	18/06/2014 13:52:10 GMT
messageDigest	17 99 17 EB E5 8D 6F B0 AD 54 19 25 9A 78 5C 80 48 0E 99 19 C7 72 A2 49 A5 D2 6E FD 58 7B 1F 07
id-aa-signingCertificateV2	sha256(D7 6E D4 51 BD 6A 7F 1A 1B BF F9 08 A3 14 B3 C3 ED 05 8B 17 8C CD 04 D6 94 26 0D 23 0E 27 A8 B2) issuer(Postecom CA3, Postecom S.p.A., IT)
Attributi 'unsigned':	
unstructuredName	PKCS7-File-HeaderDescription=Proposta CompEd Developer License;Filename=Pro ... nitarie-21041.pdf;
id-smime-aa-timeStampToken	[marca temporale 18/06/2014 13:52:10 UTC]

3.1.3 La barra menu di DigitalSign

La barra menu principale di DigitalSign raggruppa i menu di comandi e funzioni accessibili all'utente.

La barra principale contiene le seguenti funzioni (descritte in dettaglio nella sez. 4.2 e successive)

File
Strumenti
Dispositivo di Firma
Finestre

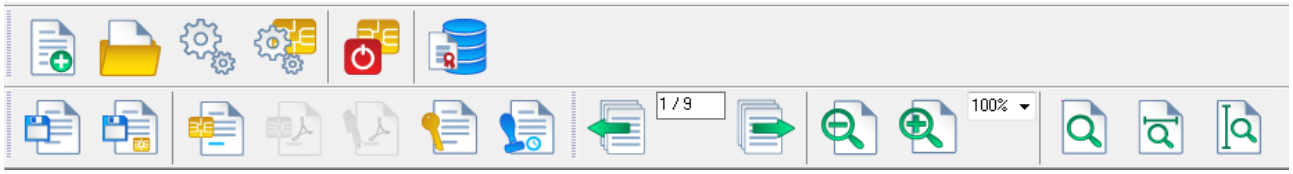
Aiuto

Quando è aperta una finestra documento può essere disponibile anche un altro menu:

Documento

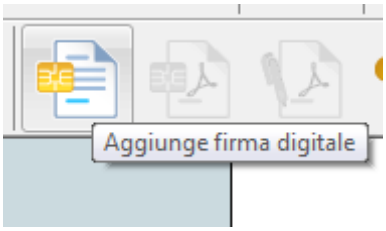
3.1.4 Le barre strumenti *(toolbar)*

Le toolbar di DigitalSign sono configurabili da parte dell'utente e contengono alcuni bottoni dall'aspetto grafico corrispondenti alle funzioni di uso più comune, normalmente accessibili attraverso il menu.



L'aspetto effettivo delle toolbar dipende dall'edizione di ***DigitalSign*** a disposizione, dalle funzioni abilitate al momento, dal tipo di documento eventualmente aperto e selezionato, dalla disponibilità o meno di un dispositivo di firma inserito, dalle caratteristiche dello stesso dispositivo.

Passando con il puntatore del mouse sopra una icona di una toolbar si visualizza un tooltip che richiama l'associata voce del menu:



Le toolbar sono configurabili attraverso il menu **Strumenti -> Opzioni**, scegliendo poi il tab **Toolbar** che conduce ad una apposita finestra di configurazione.

3.1.5 I Pannelli Informativi

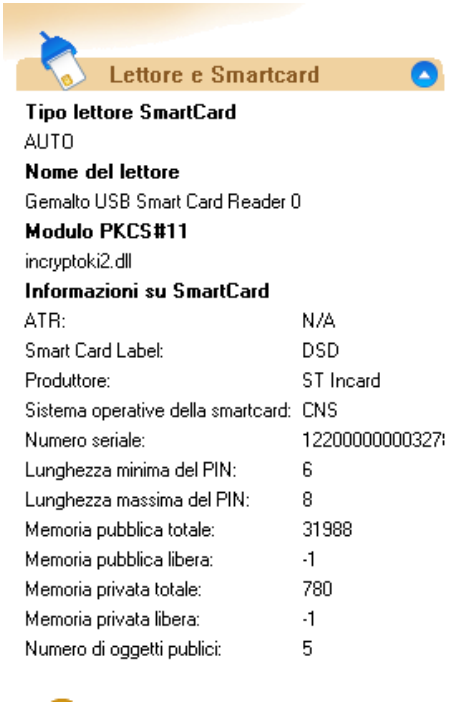
Nella finestra principale di DigitalSign possono essere visualizzati (per tramite del menu **Finestre**) alcuni pannelli di informazione, che a loro volta possono essere chiusi o aperti agendo sul simbolo a forma di freccia.

Questi pannelli consentono soltanto di visualizzare rapidamente alcune informazioni relative alla configurazione corrente del dispositivo di firma e delle opzioni di *security* impostate, ma non permettono di modificare direttamente tali informazioni.

L'illustrazione sopra riportata mostra i pannelli tutti in posizione chiusa. Operando sul simbolo a destra è possibile aprire (o richiudere) tutti i pannelli.

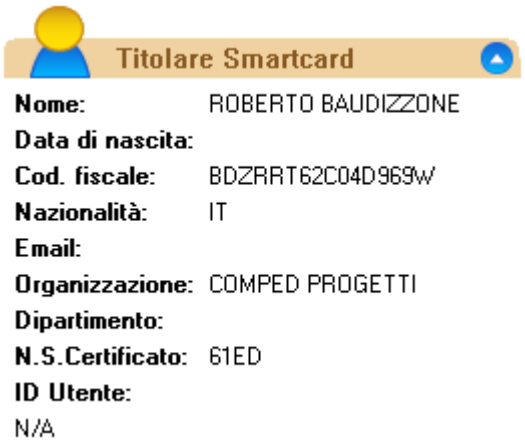
I pannelli disponibili sono:

- **Lettore e smartcard**



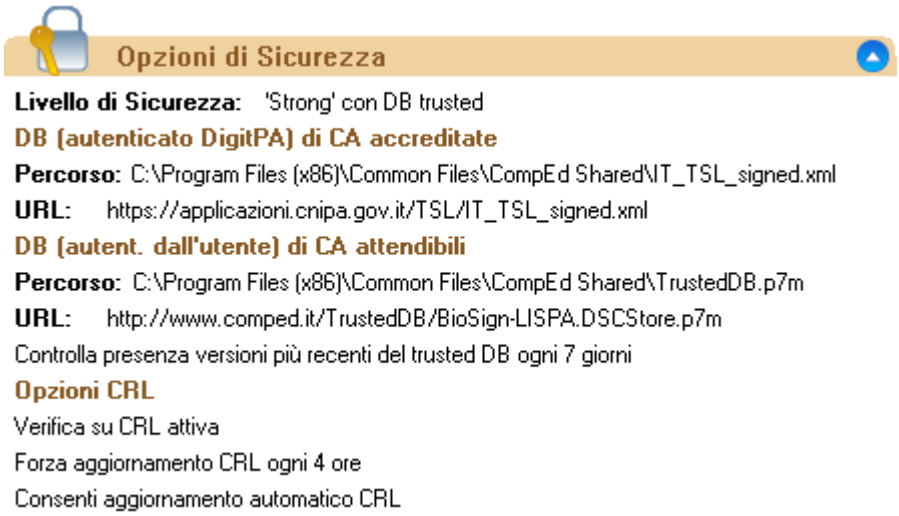
Questo pannello mostra alcuni dettagli relativi al lettore di smartcard correntemente attivo, all'eventuale modulo PKCS#11 tramite cui avviene il collegamento al dispositivo, alla particolare smartcard inserita nel lettore

- **Titolare Smartcard**



Questo pannello mostra alcuni dettagli sull'identità del titolare del dispositivo di firma correntemente inserito nel lettore. I dati visualizzati sono estratti dal certificato letto dal dispositivo stesso.

- **Opzioni di Sicurezza**


Opzioni di Sicurezza
Livello di Sicurezza: 'Strong' con DB trusted
DB (autenticato DigitPA) di CA accreditate
Percorso: C:\Program Files (x86)\Common Files\CompEd Shared\IT_TSL_signed.xml
URL: https://applicazioni.cnipa.gov.it/TSL/IT_TSL_signed.xml
DB (autent. dall'utente) di CA attendibili
Percorso: C:\Program Files (x86)\Common Files\CompEd Shared\TrustedDB.p7m
URL: http://www.comped.it/TrustedDB/BioSign-LISPA.DSCStore.p7m
Controlla presenza versioni più recenti del trusted DB ogni 7 giorni
Opzioni CRL
Verifica su CRL attiva
Forza aggiornamento CRL ogni 4 ore
Consenti aggiornamento automatico CRL

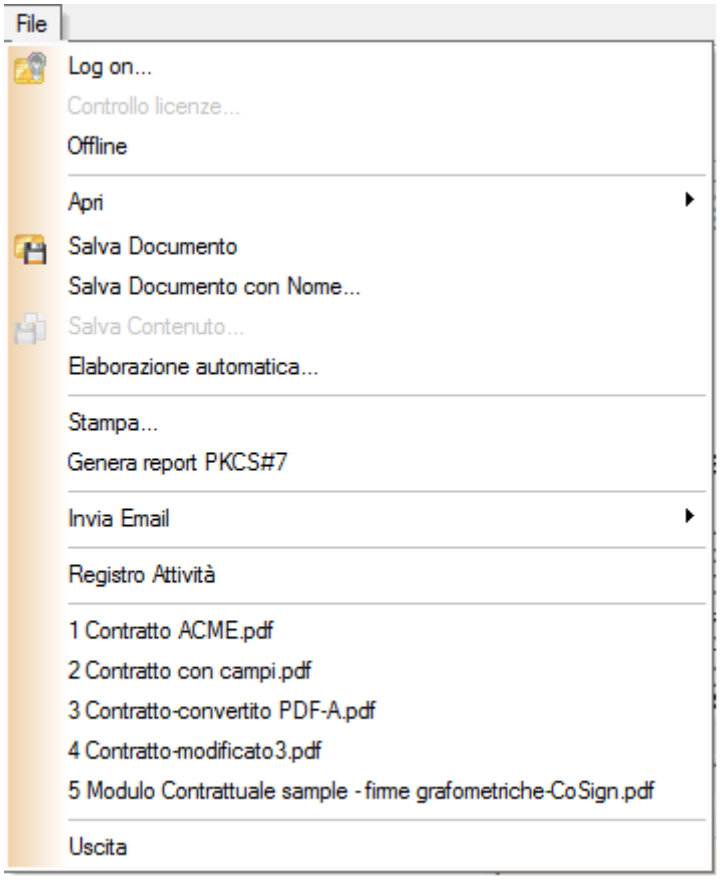
Questo pannello mostra le informazioni principali relativamente alle opzioni di *security* correntemente attive.
Per modificare la configurazione di tali opzioni si utilizza il menu **Strumenti -> Opzioni di Security**

3.1.6 La barra di stato

La barra di stato principale di DigitalSign viene mostrata alla base della finestra principale dell'applicazione

Come si può notare la status bar principale mostra informazioni relative allo stato di funzionamento di DigitalSign, alla modalità di gestione dell'interfaccia al dispositivo di firma, al titolare del dispositivo di firma correntemente inserito, allo stato di *Logon* o di *Logoff* del dispositivo stesso.

3.2 Il menu "File"



Questo menu contiene diverse funzioni, alcune delle quali possono non essere disponibili, per esempio se nessun documento è aperto.
Oltre alle funzioni descritte nelle sezioni seguenti, è di norma presente – come illustrato in figura – anche una lista di elementi corrispondenti agli ultimi 5 documenti elaborati, utili per aprire in modo immediato un documento utilizzato di recente.

Gli elementi di menu sono visualizzati accanto al simbolo dell'eventuale icona della barra strumenti che esegue la stessa funzione.

3.2.1 Log On / Log Off

Funzione non disponibile con DigitalSign Reader

Questa funzione di menu consente di porre il dispositivo di firma (la smartcard) in uno stato di "Log On", ossia di attivarne tutte le funzioni previa introduzione del proprio codice riservato, mediante una apposita finestra di dialogo.

La funzione non è utilizzabile se nessun dispositivo di firma è inserito.

Se il dispositivo è già in tale stato di Logon questa funzione lo pone in stato di Logoff, disattivandone le funzioni.

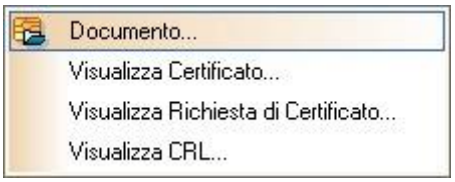
La voce di menu mostra la dicitura **Log On** se il dispositivo è disattivo, oppure **Log Off** se il dispositivo già è attivo.

3.2.2 Controllo licenze

Questa funzione è abilitata soltanto nelle edizioni di DigitalSign fornite in package con altri prodotti CompEd, come Legal Document System ®, o più in generale nei contesti in cui esiste un sistema centralizzato di controllo della licenza d'uso (CompEd License Manager).

Scopo di questa funzione è visualizzare lo stato della licenza d'uso.

3.2.3 Il sottomenu "Apri"



Questo sottomenu conduce ad alcune funzioni specifiche per aprire/visualizzare documenti di diverso tipo

3.2.3.1 Documento

Presenta una finestra di dialogo standard per la selezione di un file da aprire.
La posizione di partenza per la selezione del file dipende dalle impostazioni dei percorsi di lavoro, configurabili tramite il menu **Strumenti -> Opzioni** ed agendo sul tab **Percorsi**.

Se si apre un documento già in formato di busta crittografica allora il documento viene aperto così come si trova; se invece si apre un documento "normale" (es. PDF, DOC, TXT, JPG, ecc.) si creerà una nuova busta crittografica contenente tale documento, pronto per le successive operazioni di firma, cifratura, marcatura temporale, ecc.

Si noti che questa funzione ha un comportamento flessibile: applicandola a documenti di tipologia particolare per DigitalSign (es. Certificati, Liste di Sospensione e revoca, ecc.) essi verranno aperti con gli appropriati moduli di presentazione, non nella finestra documento, esattamente come se venissero usate le funzioni descritte nelle prossime sezioni.

3.2.3.2 Visualizza certificato

Permette di visualizzare il contenuto di un certificato, previa selezione del file, attraverso il modulo standard di visualizzazione.

3.2.3.3 Visualizza Richiesta di Certificato

Permette di visualizzare il contenuto di una Richiesta di Certificato PKCS#10, previa selezione del file, attraverso lo stesso modulo standard di visualizzazione che normalmente si usa per visualizzare il contenuto di un certificato.

3.2.3.4 Visualizza CRL

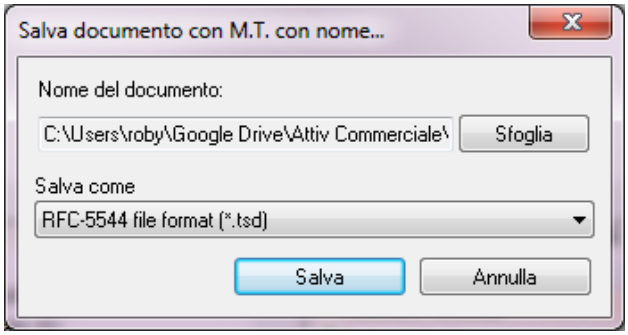
Permette di visualizzare il contenuto di una Lista di Sospensione e Revoca disponibile su un file, attraverso uno specifico modulo di visualizzazione.

3.2.4 Salva Documento

Permette di salvare il documento su cui si sta lavorando.
Poiché DigitalSign consente una gestione differenziata dei documenti in formato CAdES e PAdES, il comportamento può essere diverso secondo il tipo di file su cui si sta lavorando:

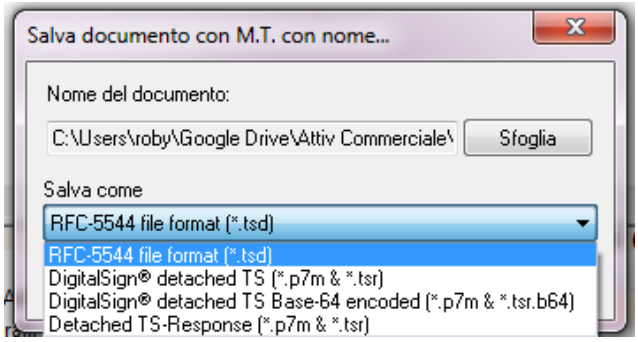
- Se si tratta di un documento DIVERSO dal formato PDF allora si salverà un file in formato .p7m (CAdES), anche se non è stata apposta alcuna firma
- Se si tratta di un documento PDF su cui non è stata apposta alcuna firma si salverà ancora in formato PDF
- Se si tratta di un documento PDF su cui è stata apposta una firma PAdES allora si salverà ancora in formato PDF
- Se si si tratta di un documento PDF su cui è stata apposta una firma CAdES allora si salverà un file in formato .p7m

Se si tratta di un documento corredato di una marca temporale esterna, oppure integrata in formato RFC-5544 allora l'utente ha la possibilità di scegliere il formato di uscita e dunque anche il nome del file.
L'utente vedrà una finestra di dialogo di questo genere:



L'utente può usare il bottone Sfoglia per scegliere la posizione ed il nome del file da creare, quindi completare o annullare l'operazione.

La lista permette di scegliere tra le diverse modalità disponibili:


Salva documento con M.T. con nome...
Nome del documento:
C:\Users\roby\Google Drive\Attiv Commerciale\
Sfoglia
Salva come
RFC-5544 file format (*.tsd)
RFC-5544 file format (*.tsd)
DigitalSign® detached TS (*.p7m & *.tsr)
DigitalSign® detached TS Base-64 encoded (*.p7m & *.tsr.b64)
Detached TS-Response (*.p7m & *.tsr)

Per una descrizione delle diverse modalità si veda la sezione relativa.

Se il documento non era ancora stato salvato in precedenza il sistema presenta una finestra di dialogo standard per l'impostazione del nome del file su cui scrivere. La posizione di partenza per la selezione del file dipende dalle impostazioni dei percorsi di lavoro, configurabili tramite il menu **Strumenti -> Opzioni** ed agendo sul tab **Percorsi.**

Se il file destinazione è già esistente DigitalSign lo salva direttamente (cioè non chiede il nome), ma nel caso – probabile – che il file sia già esistente chiede conferma della volontà di sovrascriverlo.

3.2.5 Salva Documento con Nome

Funzione assolutamente analoga alla precedente, ma permette di scrivere un file di nome differente rispetto all'originale.

3.2.6 Salva Contenuto

Questa funzione consente di salvare su disco una copia del documento contenuto nella busta crittografica su cui si sta operando (non applicabile al caso di un documento PAdES, in cui non esiste una vera e propria busta crittografica).

Se, per esempio, l'utente apre il documento **`proposta_di_contratto.pdf.p7m`**, ossia un documento in formato **pdf** firmato digitalmente e quindi racchiuso in una busta crittografica PKCS#7, questa funzione permette di salvare una copia del documento **`proposta_di_contratto.pdf`**.

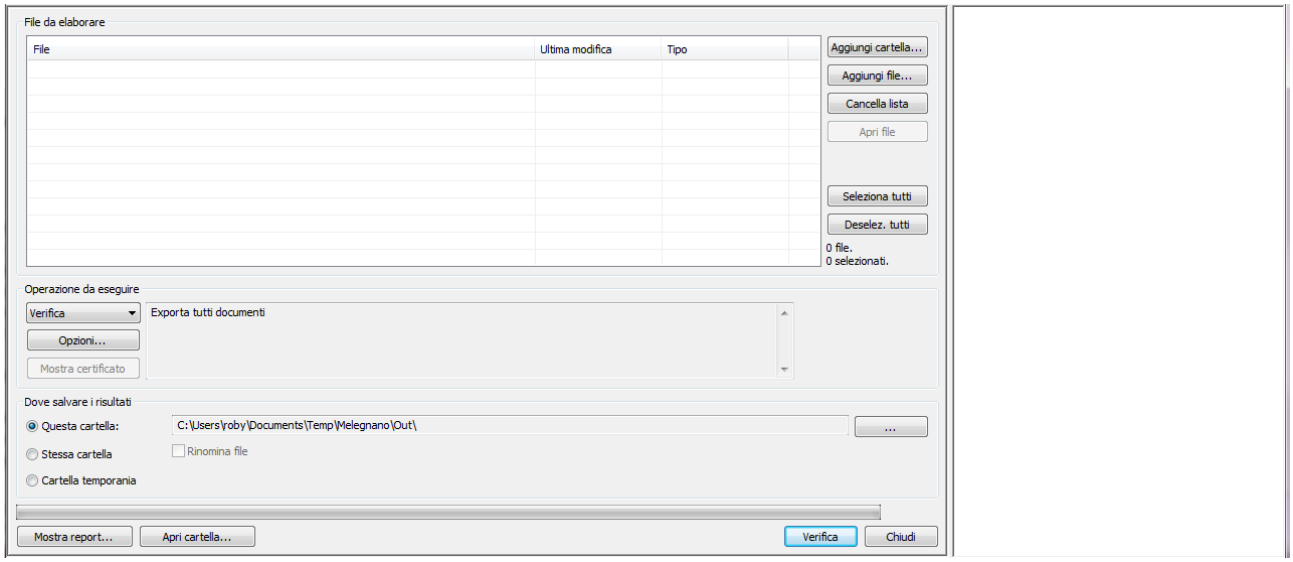
Il sistema presenta una finestra di dialogo standard per l'impostazione del nome del file su cui scrivere. La posizione di partenza per la selezione del file dipende dalle impostazioni dei percorsi di lavoro, configurabili tramite il menu **Strumenti -> Opzioni** ed agendo sul tab **Percorsi.**

3.2.7 Elaborazione Automatica

Funzione non disponibile con DigitalSign Reader

Questa funzione consente di applicare operazioni di firma, verifica, marcatura temporale, cifratura, decifratura su un intero lotto di documenti.

Inizialmente l'applicazione presenta una schermata di questo tipo:



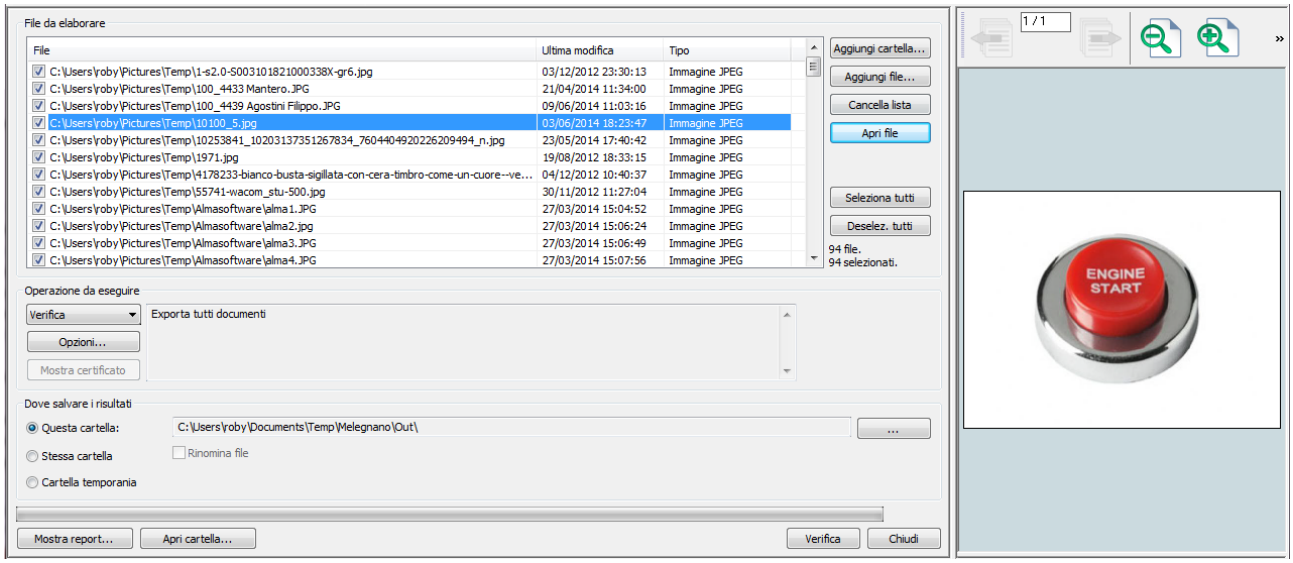
Il riquadro, inizialmente vuoto, conterrà i documenti a cui applicare l'operazione automatica prescelta.
La prima cosa da fare è popolare la lista. Per questo si usano i seguenti comandi:

- **Aggiungi Cartella** – con questo comando possiamo aggiungere alla lista l'intero contenuto di una cartella specificata
- **Aggiungi File** – con questo comando l'utente può selezionare uno o più file da includere nella lista

Si noti che la funzione *drag&drop* di Windows consente di trascinare documenti da una finestra di Wndows Explorer e lasciarli nella lista, ottenendo lo stesso risultato di **Aggiungi File**.

Questi comandi possono essere usati più volte, aggiungendo diversi documenti ad ogni passo.
Il comando **Cancella Lista** permette di svuotare l'intera lista in un click.

Dopo aver popolato la lista vedremo qualcosa del genere:

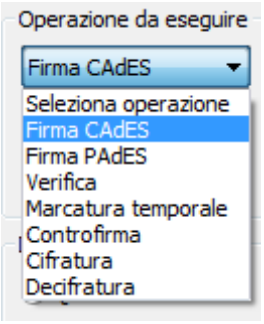


Si noti che il riquadro anteprima presenta il contenuto del singolo file su cui eventualmente posizioniamo il cursore, così da permettere l'effettiva visualizzazione di qualunque documento prima di firmarlo.

Si noti anche che tutti i file caricati hanno, a sinistra, una casella di spunta. Inizialmente sono TUTTI selezionati, ma l'utente può clikkare su ciascuna casella per invertire lo stato selezionato/non selezionato: il ciclo di elaborazione automatica agirà SOLTANTO sui documenti SELEZIONATI.

I bottoni comando **Seleziona tutti** e **Deseleziona tutti** permettono di agire in un solo click sullo stato di selezione dell'intera lista.

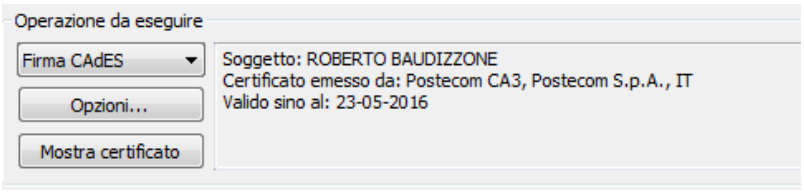
Dopo aver determinato la lista di documenti su cui vogliamo agire occorre decidere quale operazione eseguire.



In funzione dell'operazione scelta dovremo impostare alcuni parametri specifici:

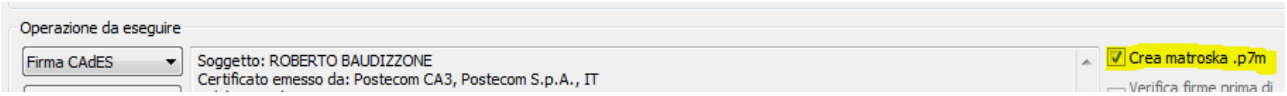
3.2.7.1 Firma CAdES

Appena scelta questa opzione il sistema chiede il logon al dispositivo di firma e visualizza nel riquadro accanto al bottone comando i dati del certificato che verrà usato per la firma:



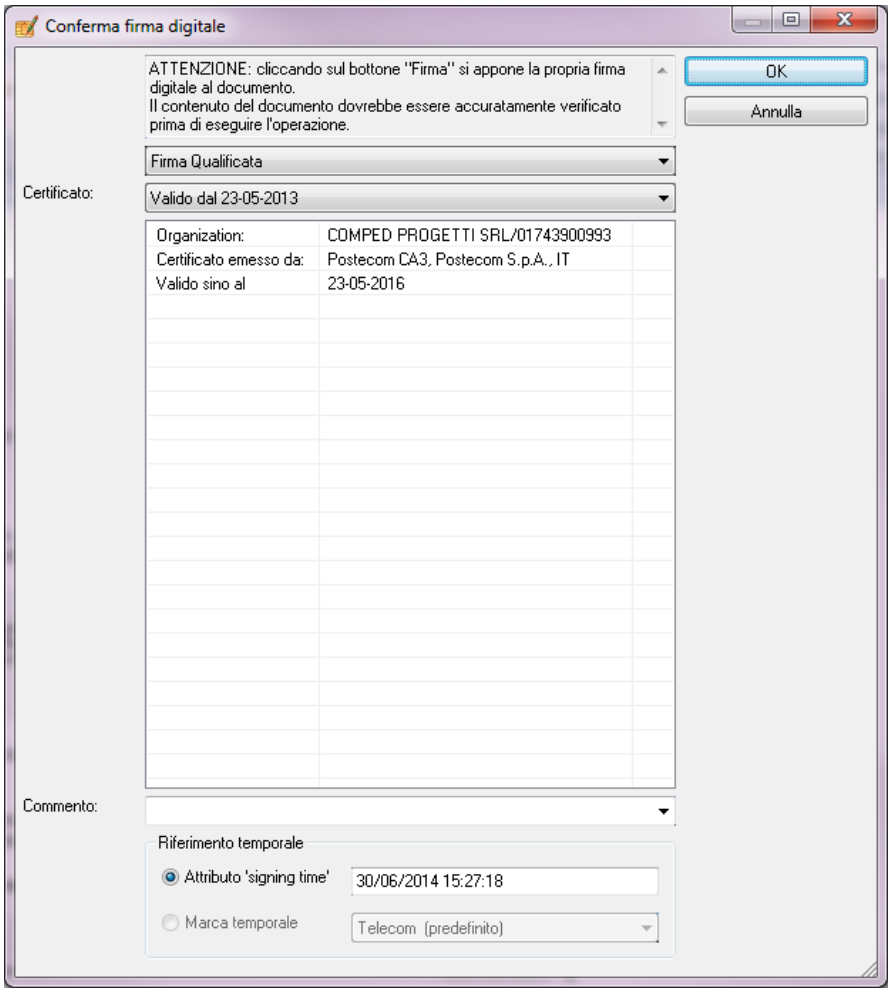
Il bottone Mostra Certificato permette di visualizzare i dettagli del certificato stesso, con la consueta finestra di dialogo.

Si noti che la firma CAdES può applicarsi a qualunque tipo di file; se un file da firmare è già in formato CAdES il sistema appone una ulteriore firma in modo parallelo a quella/quelle eventualmente già presenti, nella stessa busta crittografica.
Ma è possibile spuntare il checkbox **Crea matrioska .p7m**:



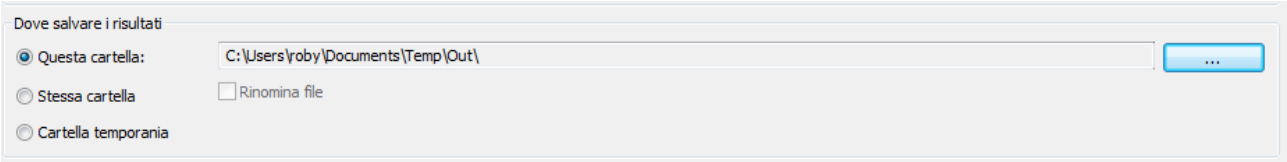
In questo caso se il documento è già un .p7m si creerà comunque una ulteriore busta crittografica esterna con la nuova firma.

Facendo click su **Opzioni** si aprirà la stessa finestra di dialogo di conferma di una firma CAdES, utilizzata anche nel caso di firma di un singolo documento:


Conferma firma digitale
ATTENZIONE: cliccando sul bottone "Firma" si appone la propria firma digitale al documento.
Il contenuto del documento dovrebbe essere accuratamente verificato prima di eseguire l'operazione.
OK
Annulla
Firma Qualificata
Certificato:
Valido dal 23-05-2013
Organization: COMPED PROGETTI SRL/01743900993
Certificato emesso da: Postecom CA3, Postecom S.p.A., IT
Valido sino al 23-05-2016
Commento:
Riferimento temporale
Attributo 'signing time' 30/06/2014 15:27:18
Marca temporale
Telecom (predefinito)

Qui possiamo scegliere tra le diverse opzioni di firma, se ne esistono più di una, oltre che tra l'uso di un riferimento temporale *"signing time"* (ora proveniente dal computer) o una vera e propria marca temporale.

Quindi dovremo scegliere dove salvare i risultati:



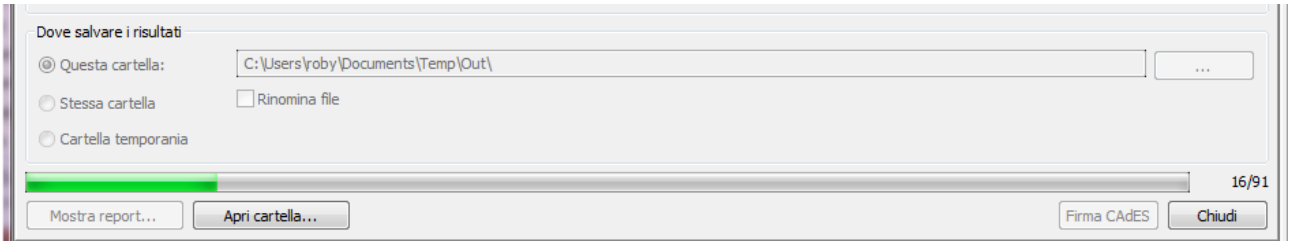
Per default si utilizza una cartella specificamente destinata a contenere il risultato, da impostare mediante il bottone

In alternativa si può usare la **stessa cartella** in cui si trova il file origine (del caso rinominando il file di destinazione, aggiungendo al nome il suffisso "`-firmato`", oppure usare la **Cartella Temporanea** standard di Windows.

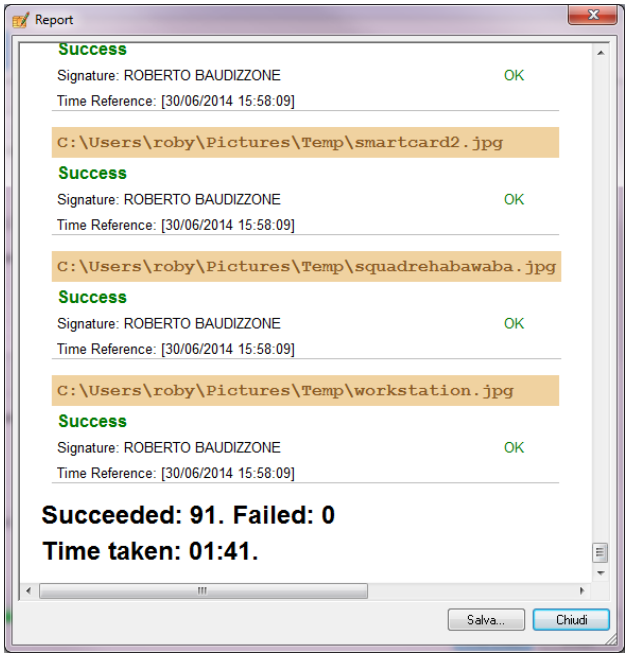
Si noti che se nella cartella di destinazione esiste già un file con il nome che assumerà il risultato, automaticamente il nuovo file sarà rinominato con il suffisso "-1", "-2", ecc.

Dopo che tutto è definito si agisce sul bottone **Elabora** per avviare effettivamente il processo:

Durante l'elaborazione l'utente vede una progress bar che avanza man mano che i documento sono elaborati:



Al termine dell'elaborazione si apre automaticamente il report dell'esecuzione:



Una volta chiusa questa finestra contenente il report possiamo riaprirla con il bottone **Mostra report**; con **Apri cartella** possiamo invece aprire direttamente la cartella contenente i file prodotti.

3.2.7.2 Firma PAdES

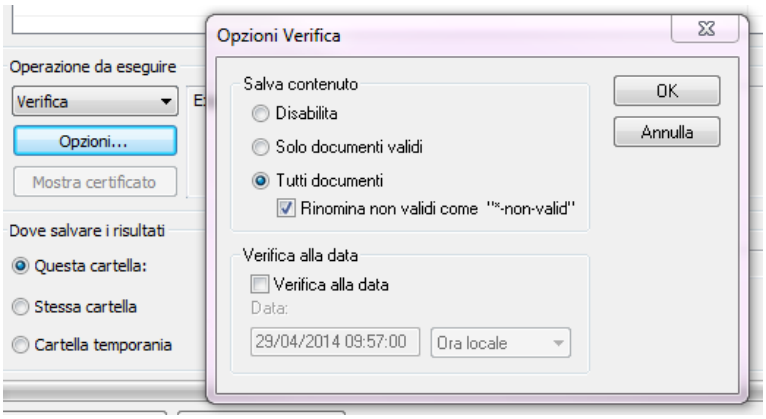
L'operazione di Firma PAdES è del tutto simile alla Firma CAdES illustrata nella sezione precedente.
Naturalmente può essere applicata soltanto a documenti PDF, quindi il tentativo di applicarla a documenti d'altro tipo produrrà un errore:

Per il resto cambia l'aspetto della schermata di conferma (**Opzioni**), per i cui dettagli si rimanda alla funzione di **Firma PAdES** su un documento.

3.2.7.3 Verifica

Questa funzione permette di verificare automaticamente le firme di una serie di documenti, ottenendo un report con i risultati della verifica di ciascuno.
Si noti che i dettagli ricavabili in questo modo non sono fini come quelli ottenuti aprendo e verificando visivamente un singolo documento, ma certamente con questa tecnica è possibile verificare in un attimo grandi quantità di documenti presenti in una cartella.

Una funzione molto interessante, per il caso di documenti CAdES, è quella del "disimbustamento automatico":



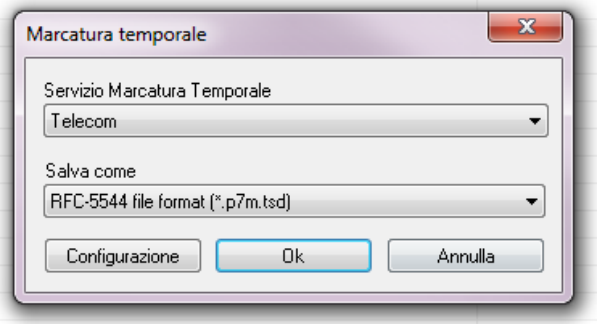
Utilizzando il bottone Opzioni si accede alla finestra di dialogo qui visualizzata. Il radio-button permette di decidere se operare in effetti il salvataggio del contenuto di un documento CAdES o meno, inoltre se farlo per tutti i documenti o solo per quelli che superano la verifica.

Il riquadro sottostante permette di impostare la "verifica alla data", in modo analogo a quanto avviene nel caso di verifica alla data di un singolo documento.

Per il resto anche nella Verifica – proprio per il caso in cui si richieda il salvataggio dei contenuti – è possibile indicare una cartella di destinazione, come nelle operazioni di firma descritte nelle sezioni precedenti.

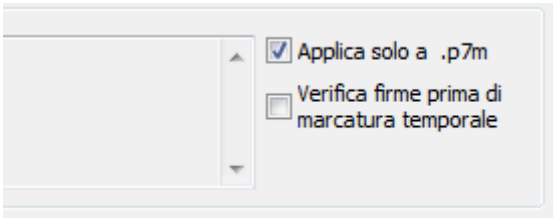
3.2.7.4 Marcatura Temporale

Questa funziona permette di applicare una marca temporale all'insieme di file selezionato nella lista.
Le opzioni prevedono:



- Scelta del **servizio di Marcatura Temporale**, tra quelli correntemente configurati
- Scelta del **formato di output** (per una descrizione delle opzioni disponibili si veda la sezione dedicata alla marcatura temporale di un singolo file.

Si noti la presenza di 2 checkbox per altrettante opzioni:

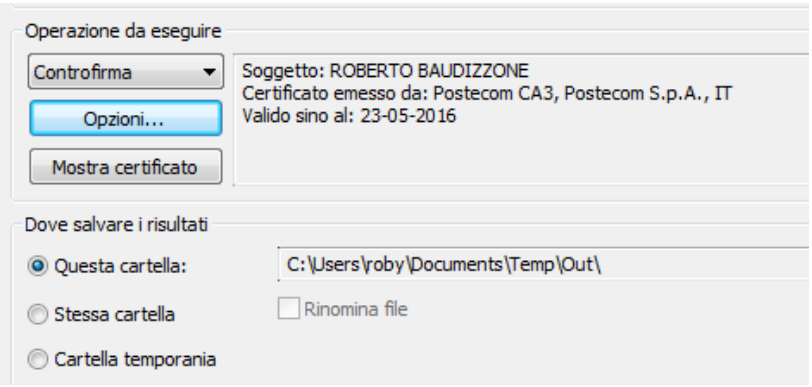


- **Applica solo a .p7m** – limita l'azione ai soli documenti di tipo .p7m
- **Verifica firme prima di marcatura temporale** – se selezionato evita che una marca temporale sia apposta ad un documento firmato che contenga almeno una firma non valida

NOTA IMPORTANTE: poiché il servizio di marcatura temporale è una risorsa soggetta a costi, è bene utilizzare usare questa funzione con attenzione. DigitalSign presenta una schermata di conferma prima di lanciare l'operazione, ricordando il numero totale di documenti selezionati per la marcatura temporale.
L'utente può disabilitare questo ulteriore avvertimento.

3.2.7.5 Controfirma

Questa funzione permette di applicare una Controfirma ad una firma già presente in un documento CAdES.
Si noti che il concetto di controfirma è applicabile solo a documenti CAdES, che contengano già almeno una firma.



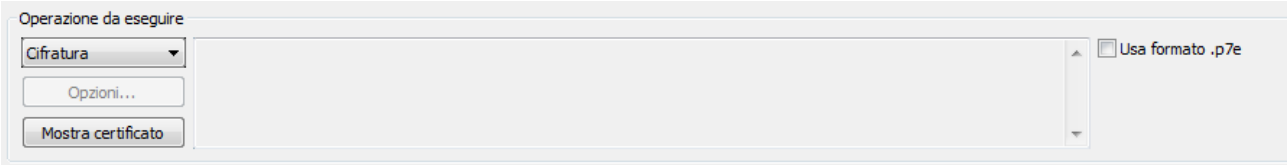
L'operatività è analoga a quella della Firma CAdES.

Normalmente, nella modalità interattiva, l'utente naviga nel pannello delle proprietà ed individua la firma già esistente a cui intende apporre una controfirma, ma in questo contesto di elaborazione automatica non è possibile agire così selettivamente.
Quindi il sistema applica una regola generale: la controfirma è apposta all'ultima firma (o controfirma) trovata nel documento.
Quindi:

- se il documento contiene una sola firma, la controfirma è apposta a tale firma
- se il documento contiene due o più firme parallele, la controfirma è apposta all'ultima della lista
- se l'ultima (o unica) firma parallela già apposta al documento presenta già uno o più livelli di controfirme, la nuova controfirma è apposta all'ultima controfirma.

3.2.7.6 Cifratura

Questa funzione permette di cifrare il lotto di documenti a beneficio di una lista di "destinatari" abilitati, individuati attraverso i rispettivi certificati di cifratura che devono essere già presenti nel DB dei certificati.



Il bottone Opzioni apre la finestra di dialogo per la selezione dei destinatari della cifratura, del tutto analogo a quello descritto a proposito della cifratura di un singolo documento.

L'opzione Usa formato .p7e influisce sul formato di uscita del documento, nel caso i documenti di partenza fossero già firmati in formato CAdES:

- se l'opzione NON è selezionata allora un singolo livello di busta crittografica conterrà sia la firma o le firme e gli elementi di cifratura (certificati dei destinatari, chiavi di sessione cifrate, ecc.); il documento manterrà la sola estensione .p7m che aveva in partenza;
- se l'opzione è selezionata allora si genera un'ulteriore busta crittografica più esterna, dedicata ai soli elementi della cifratura; il risultato sarà un documento "a matrioska", con estensione .p7m.p7e

3.2.7.7 Decifratura

Funzione "duale" rispetto alla precedente, consente di decifrare i documenti inclusi nella lista, a condizione che siano cifrati con un certificato corrispondente ad una chiave privata disponibile (tipicamente nella smartcard correntemente inserita).

Si noti che l'output di questa funzione corrisponde alla funzione Salva contenuto, quindi nel caso – ad esempio – di un documento PDF firmato e cifrato nella stessa busta si troverà nella cartella di output il solo PDF.

3.2.8 Stampa

Manda in stampa il documento su cui si sta operando.

Viene presentata una finestra di dialogo standard per il controllo del processo di stampa (scelta del dispositivo, scelta dell'intervallo di pagine, ecc.)

Si noti che la stampa ha per oggetto il documento contenuto, nel caso di busta crittografica CAdES, quindi non conterrà informazioni sulle firme e sugli altri elementi inclusi nella busta.
Inoltre la stampa è in generale affidata al sistema operativo che attiva l'applicazione associata ad ogni tipo.

Si dovrebbe considerare la funzione di stampa di DigitalSign come una mera funzione ausiliaria, senza aspettarsi particolare qualità o raffinati automatismi.
Per ottenere stampe di qualità è sempre raccomandato:

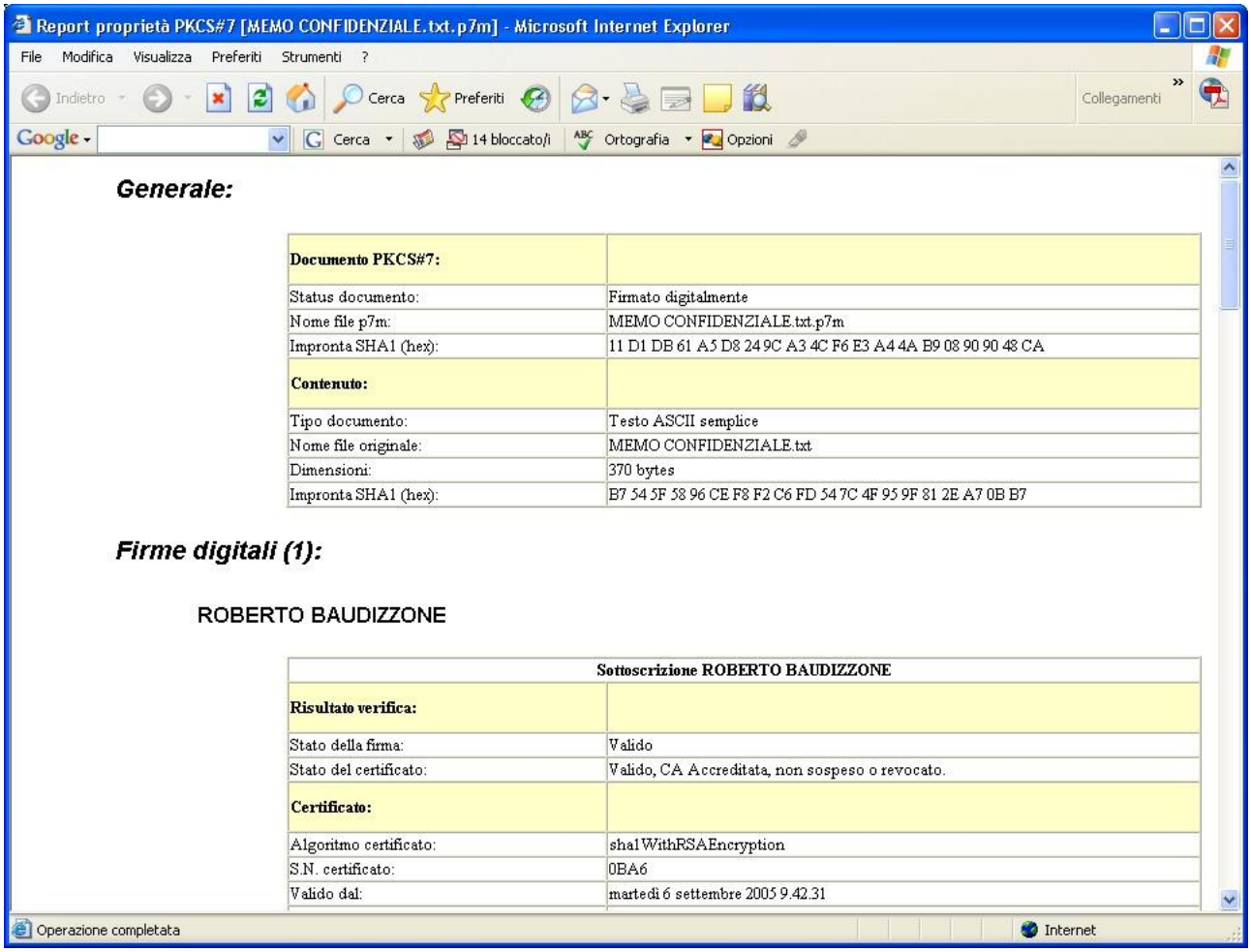
1. Esportare il contenuto del documento (nel caso CAdES) con Salva contenuto
2. Aprire il documento così ottenuto con l'applicazione associata e da lì azionare la stampa

Nel caso di documenti PAdES è sufficiente aprirli dal sistema operativo (che verosimilmente lo affiderà ad Adobe Reader) e da qui lanciare la stampa.

3.2.9 Genera Report

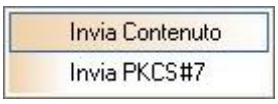
Questa funzione consente di generare un rapporto contenente tutti i dettagli relativi al documento correntemente aperto, inclusi il valore dell'impronta, la firma o le firme digitali presenti, i certificati, le marche temporali, ecc.

Questo report è costruito in formato HTML e viene successivamente aperto tramite Internet Explorer, da cui è possibile salvarlo, stamparlo, ecc.

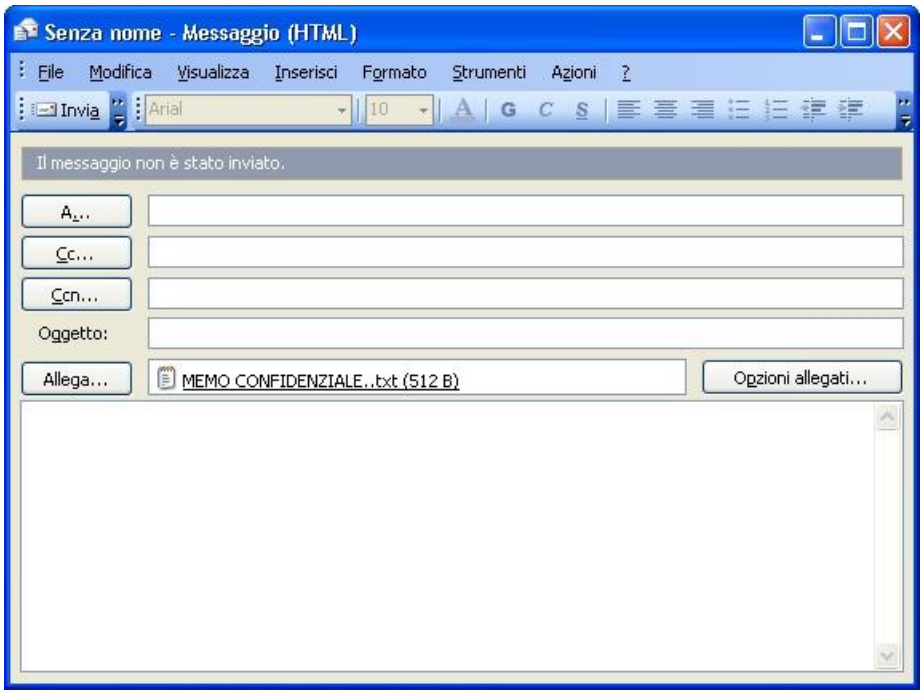

Report proprietà PKCS#7 [MEMO CONFIDENZIALE.txt.p7m] - Microsoft Internet Explorer
File Modifica Visualizza Preferiti Strumenti ?
Indietro Cerca Preferiti Collegamenti
Google Cerca 14 bloccato/i Ortografia Opzioni
Generale:
Documento PKCS#7:
Status documento: Firmato digitalmente
Nome file p7m: MEMO CONFIDENZIALE.txt.p7m
Impronta SHA1 (hex): 11 D1 DB 61 A5 D8 24 9C A3 4C F6 E3 A4 4A B9 08 90 90 48 CA
Contenuto:
Tipo documento: Testo ASCII semplice
Nome file originale: MEMO CONFIDENZIALE.txt
Dimensioni: 370 bytes
Impronta SHA1 (hex): B7 54 5F 58 96 CE F8 F2 C6 FD 54 7C 4F 95 9F 81 2E A7 0B B7
Firme digitali (1):
ROBERTO BAUDIZZONE
Sottoscrizione ROBERTO BAUDIZZONE
Risultato verifica:
Stato della firma: Valido
Stato del certificato: Valido, CA Accreditata, non sospeso o revocato.
Certificato:
Algoritmo certificato: sha1WithRSAEncryption
S.N. certificato: 0BA6
Valido dal: martedì 6 settembre 2005 9.42.31
Operazione completata
Internet

3.2.10 Il sottomenu “Invia Email”

Presenta un sottomenu con due opzioni successive:



È necessario che sul sistema sia impostato un client predefinito di posta elettronica; tramite tale client (es. **MS Outlook** ®) viene creato un nuovo messaggio di posta elettronica contenente l’oggetto selezionato come allegato.



3.2.11 Registro Attività

Funzione non disponibile con DigitalSign Reader

Consente di ispezionare il contenuto del registro delle attività, tramite un componente software separato da DigitalSign.

Per l'abilitazione/disabilitazione della funzione di registrazione degli eventi e per la configurazione sulle categorie di eventi da includere nella registrazione si usa relativa configurazione si usa il menu **Strumenti -> Opzioni** agendo quindi sul tab **Registro Attività**

3.2.12 Uscita

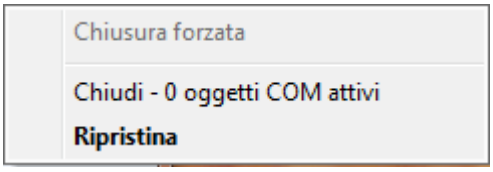
Questa funzione provoca la chiusura dell'applicazione.

Si noti che la normale azione su questo comando (o sul simbolo di chiusura della finestra principale dell'applicazione) DigitalSign non viene del tutto scaricato dalla memoria e resta quindi pronto per una rapida riattivazione. Questo stato è testimoniato dalla presenza dell'icona di DigitalSign nella *system tray*:

Lo scaricamento dalla memoria avviene spontaneamente dopo qualche minuto di completa inattività di DigitalSign (considerando anche il fatto che altre applicazioni potrebbero utilizzarne i servizi), oppure:

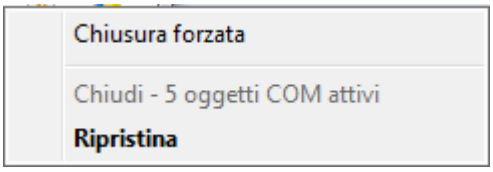
- tenendo premuto il tasto SHIFT quando si attiva questo comando di uscita (o si clicca sul bottone di chiusura della finestra);

- facendo click con il tasto destro sull'icona di DigitalSign presente nella *system tray* dopo la chiusura normale dell'applicazione ed operando sul pop-up menu che appare:



Come si può notare, l'opzione **Chiusura forzata** è disabilitata, perché non necessaria. Da qui si può usare l'opzione **Chiudi – 0 oggetti COM attivi**, perché non esistono altri processi che necessitano di DigitalSign in funzione.

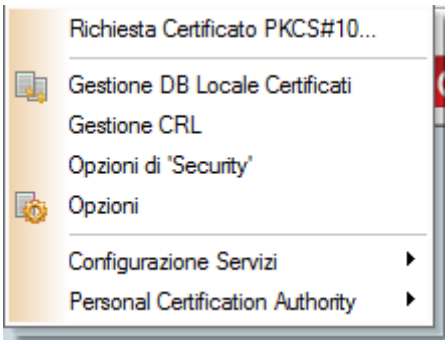
Se invece qualche applicazione stesse usando DigitalSign lo stesso menu si presenterebbe in una forma del genere:



Stavolta è l'opzione **Chiudi** ad essere disabilitata (pur mostrando il numero di oggetti COM aperti da altre applicazioni).
La chiusura sarebbe dunque possibile solo con la **Chiusura forzata**, tenendo presente che questo potrebbe avere effetti negativi sulle altre applicazioni aperte.

In entrambi i casi **Ripristina** riattiva la finestra principale di DigitalSign.

3.3 Il menu "Strumenti"



Il menu **Strumenti** raccoglie diverse funzioni di servizio ed utili alla configurazione del sistema.

Alcune voci conducono ad ulteriori sottomenu.

3.3.1 Richiesta di certificato PKCS#10

Questa funzione non è disponibile in DigitalSign Reader
Inoltre può essere disabilitata in alcune edizioni Professional OEM distribuite da alcune importanti organizzazioni.

Questa funzione viene di regola utilizzata nei contesti di utilizzo sperimentale o comunque in un gruppo chiuso di utenti, quando non si intende utilizzare smartcard fornite da un Certificatore Accreditato.
In tali casi si istituisce una funzione di *Certification Authority* che emette certificati per gli altri utenti; questi ultimi devono dal canto loro provvedere alla generazione delle coppie di chiavi sui propri dispositivi e quindi produrre, appunto, le relative "Richieste di Certificato" attraverso questa funzione.

Per le modalità d'uso della ***Personal Certification Authority*** e di questa specifica funzione si faccia riferimento alla Guida specifica, da richiedere a CompEd.

3.3.2 Gestione DB Locale dei Certificati

Questa voce di menu consente di accedere al modulo di gestione del DB dei Certificati. A tale modulo è dedicata una specifica sezione di questo manuale, cui si rimanda: si veda la sezione dedicata.

3.3.3 Gestione CRL

Questa voce di menu consente di accedere al modulo di gestione delle Liste di Sospensione e Revoca (CRL). A tale modulo è dedicata una specifica sezione di questo manuale, cui si rimanda: si veda la sezione dedicata.

3.3.4 Opzioni di Security

Questa voce di menu consente di accedere al modulo di gestione delle Opzioni di Sicurezza, prevalentemente dedicato alle impostazioni per la verifica di firme e certificati. A tale modulo è dedicata una specifica sezione di questo manuale, cui si rimanda: si veda la sezione dedicata.

3.3.5 Opzioni

Questa voce di menu consente di accedere al modulo di gestione delle Opzioni, attraverso il quale si impostano gran parte dei parametri di configurazione di DigitalSign. A tale modulo è dedicata una specifica sezione di questo manuale, cui si rimanda: si veda la sezione dedicata.

3.3.6 Il sottomenu "Configurazione Servizi"

Questa voce conduce ad ulteriore sottomenu:

- Il primo elemento di questo sottomenu apre il modulo di configurazione degli elenchi di certificati in linea LDAP, si veda la sezione dedicata.

- Il secondo elemento conduce alla configurazione dei servizi di marcatura temporale, si veda la sezione dedicata.
  Funzione non disponibile in DigitalSign Reader

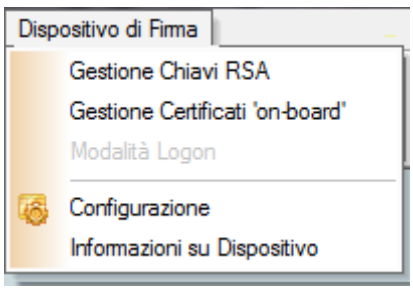
3.3.7 Personal Certification Authority

Questa funzione – insieme a tutte le funzioni del relativo sottomenu - non è disponibile in DigitalSign Reader. Inoltre può essere disabilitata in alcune edizioni Professional OEM distribuite da alcune importanti organizzazioni.

NOTA: CompEd ha realizzato una specifica guida, separata da questo manuale utente, per assistere l'utente nell'utilizzo della ***Personal Certification Authority***. È possibile richiederle tale guida direttamente a CompEd.

3.4 Il menu "Dispositivo di Firma"

Questo menu non è disponibile con DigitalSign Reader.
Ogni specifica funzione è in ogni caso abilitata solo se è inserito un dispositivo di firma compatibile con la funzione stessa.



Questo menu raccoglie alcune funzioni di gestione dell'interfacciamento con i dispositivi di firma (smartcard, token USB, ecc.) e dei relativi contenuti.

3.4.1 Gestione Chiavi RSA

Un dispositivo di firma contiene, tra gli altri oggetti, coppie di chiavi RSA.
Questa funzione permette di esaminare le chiavi attualmente contenute nel dispositivo, ed eventualmente di intervenire con operazioni di creazione, eliminazione, importazione, esportazione.

I dettagli operativi sono descritti in una sezione dedicata.

3.4.2 Gestione Certificati 'on-board'

Un dispositivo di firma di norma contiene chiavi e certificati.
Questa funzione permette di accedere al Modulo di Gestione di questi certificati, offrendo in generale opzioni per la visualizzazione e l'esportazione di questi certificati.
Se il particolare dispositivo lo permette è anche possibile caricare certificati nella memoria del dispositivo.

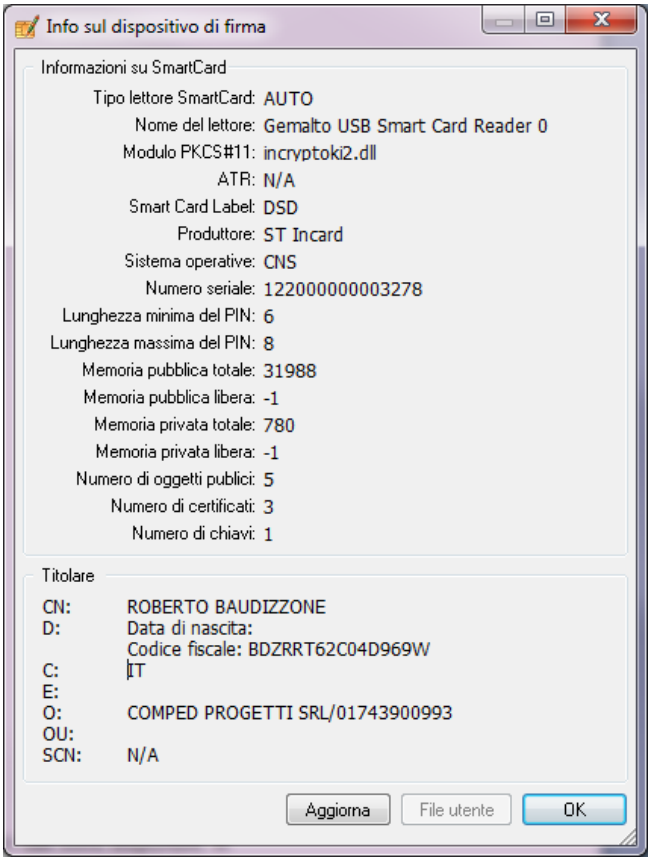
I certificati *on-board* sono particolarmente importanti perché considerati intrinsecamente attendibili in fase di verifica di firme e certificati.

3.4.3 Configurazione

Questa importante funzione serve a controllare la modalità di interfacciamento tra DigitalSign ed il dispositivo di firma.
Per i dettagli si veda la sezione dedicata.

3.4.4 Informazioni sul Dispositivo

Presenta una schermata di informazioni sul dispositivo di firma correntemente inserito.

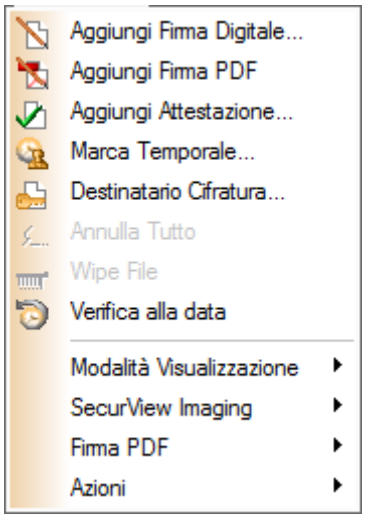


- il bottone **Aggiorna** permette di rileggere i dati dal dispositivo ed aggiornare la visualizzazione

- il bottone **OK** chiude la finestra

3.5 Il menu "Documento"

Questo menu può avere elementi diversi secondo il tipo di documento su cui si sta operando; la figura che segue mostra il caso più completo:



Questo menu è visibile solo quando almeno è presente almeno una finestra documento e di norma contiene uno o più sottomenu.

3.5.1 Aggiungi Firma CAdES

Funzione non disponibile con DigitalSign Reader

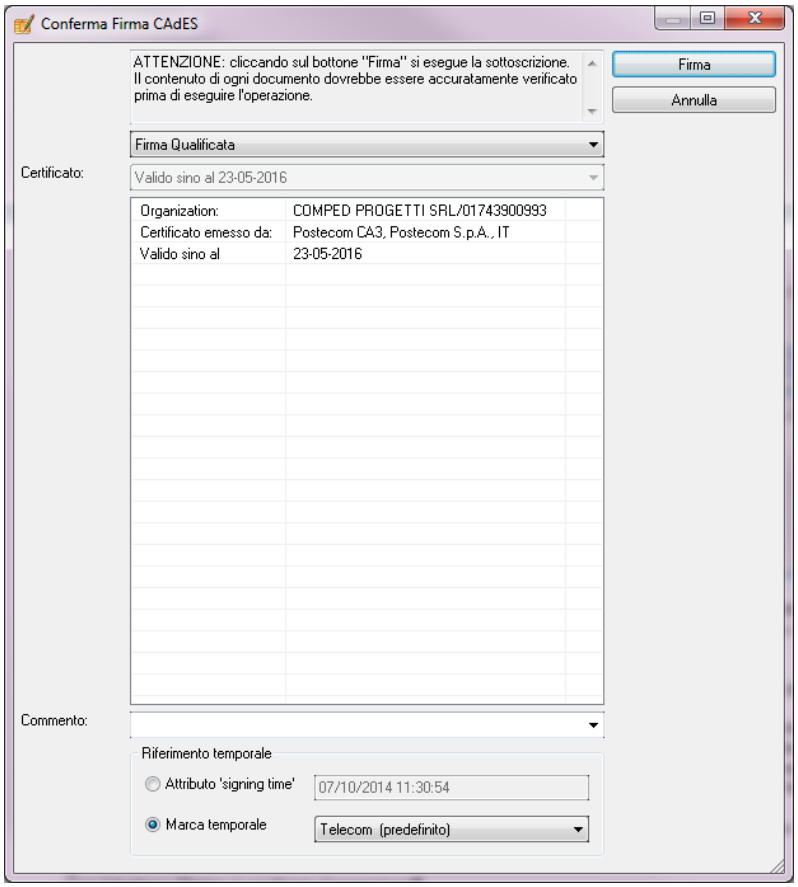
Consente di firmare digitalmente il documento aperto correntemente selezionato, se è disponibile un dispositivo di firma idoneo e se il documento non contiene ancora una firma digitale (CAdES) corrispondente allo stesso certificato.

ATTENZIONE: se il documento aperto è di tipo PDF "semplice", ancora non firmato (prima di scegliere un tipo di firma), usando questa funzione si produce un file in formato CAdES. Se l'intenzione è invece di produrre un PDF firmato (PAdES) senza imbustarlo in una envelope PKCS#7, allora bisogna usare la funzione Aggiungi firma PDF.

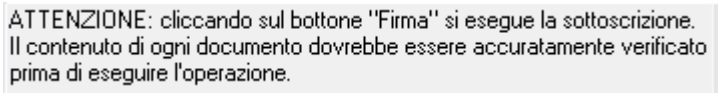
Questa funzione non è disponibile se il documento aperto è tipo PDF e già contiene una o più firma in formato PAdES.

Se il documento è già firmato digitalmente l'operazione aggiunge una ulteriore firma di tipo "parallelo".

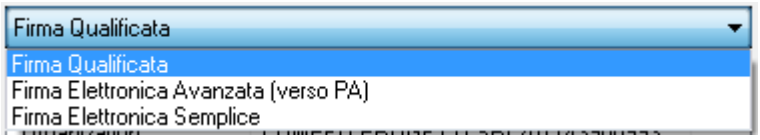
Se il dispositivo non è ancora in stato di *Logon* il sistema presenta innanzitutto la finestra di dialogo relativa, quindi quella specifica per la conferma della firma:



- In alto è riportato un testo informativo che invita l'utente a verificare accuratamente il contenuto del documento.0


ATTENZIONE: cliccando sul bottone "Firma" si esegue la sottoscrizione.
Il contenuto di ogni documento dovrebbe essere accuratamente verificato
prima di eseguire l'operazione.

- Subito sotto compare un selettore per la fattispecie di firma da apporre:

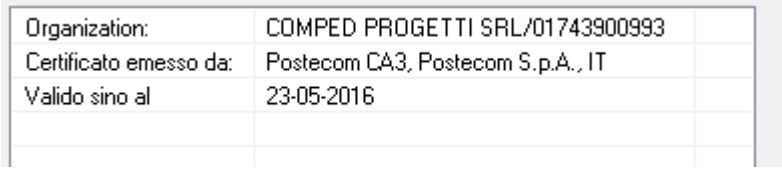


La fattispecie applicata dipende essenzialmente dalla chiave e dal certificato impiegato. Di solito si userà il certificato qualificato e si produrrà una Firma Qualificata, la fattispecie a massimo valore probatorio.
Tuttavia la normativa più recente chiarisce che utilizzando il certificato di autenticazione contenuto nelle CNS (talvolta non ci sono altri certificati, come nelle "carte cittadino" rilasciate da alcune regioni) la firma prodotta ha valore di Firma Elettronica Avanzata se usata nei confronti della Pubblica Amministrazioni.
I certificati di autenticazione o cifratura presenti invece su smartcard non CNS possono produrre Firme Elettroniche Semplici.

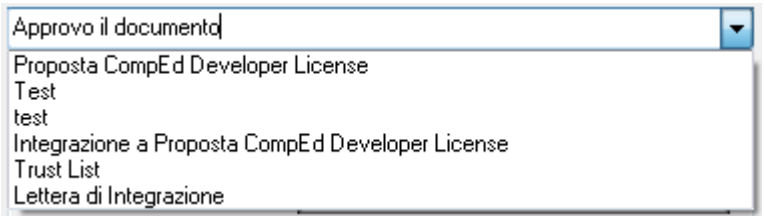
- In base alla fattispecie di firma selezionata al punto precedente appare l'indicazione del certificato correntemente selezionato:

Se la carta contenesse più di un certificato atto allo scopo la lista sarebbe selezionabile per individuare il certificato prescelto. Altrimenti (come nel caso in figura) la lista è bloccata sull'unico certificato.

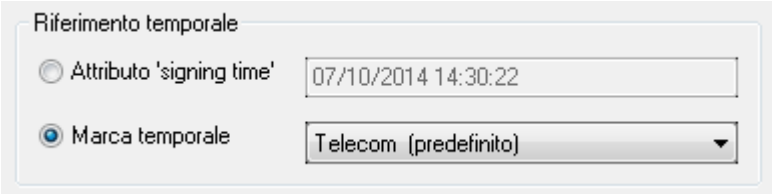
- Segue un riquadro che riassume i dati del certificato correntemente selezionato:



- Il campo Commento: qui l'utente può scrivere un commento alla firma, con la possivbilità – grazie alla lista – di richiamare i commenti inseriti in precedenza



- Infine si sceglie il tipo di riferimento temporale.



Le opzioni sono:

- **Attributo Signing Time –** scegliendo questa opzione si associa alla firma un attributo (signed, ossia coperto a sua volta dalla firma) che rappresenta la dichiarazione della data ed ora a cui viene apposta la firma. DigitalSign compila questo campo con l'ora di sistema, ma l'utente è tecnicamente libero di modificarlo (si tratta di una diretta responsabilità del sottoscrittore, appunto.
- **Marca Temporale –** scegliendo questa opzione DigitalSign genera la firma, dopo di che richiede – al servizio configurato – una marca temporale calcolata sulla firma stessa.

Con il bottone

si conferma l'operazione

Con il bottone

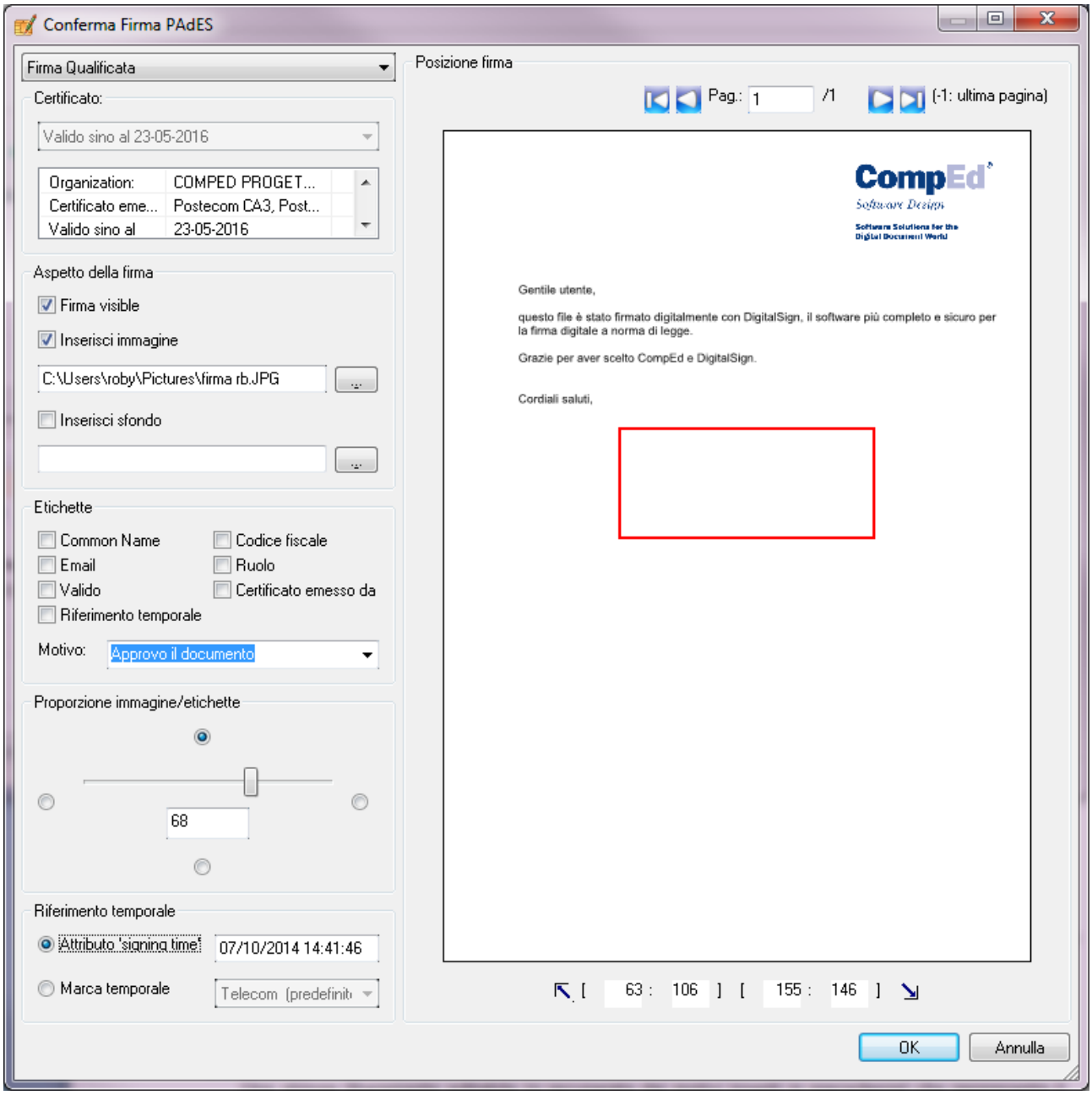
si chiude senza generare la firma

3.5.2 Aggiungi Firma PDF

Funzione non disponibile con DigitalSign Reader

Se il documento aperto è di tipo PDF e non è già in formato CAdES, questa funzione consente di apporre una firma digitale all'interno dello stesso file PDF.

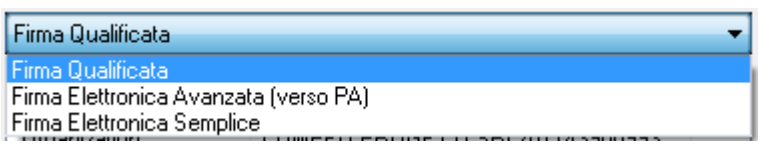
Se il dispositivo non è ancora in stato di *Logon* il sistema presenta innanzitutto la finestra di dialogo relativa, quindi quella specifica per la conferma della firma:



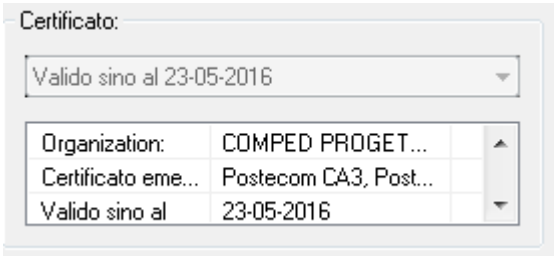
Il processo di apposizione di una firma PAdES è un po' più laboriosa rispetto a quella CAdES, perché una peculiarità di questo formato è proprio quella di consentire l'inserimento di un elemento grafico e di una lista di elementi testuali (ricavati dal certificato) all'interno del documento stesso.
Peraltro molti controlli agiscono come nel caso precedente, quindi rimanderemo direttamente alla sezione firma CAdES per una spiegazione dettagliata.

Vediamo gli elementi di questa finestra di dialogo:

- **Selettore della fattispecie di firma**

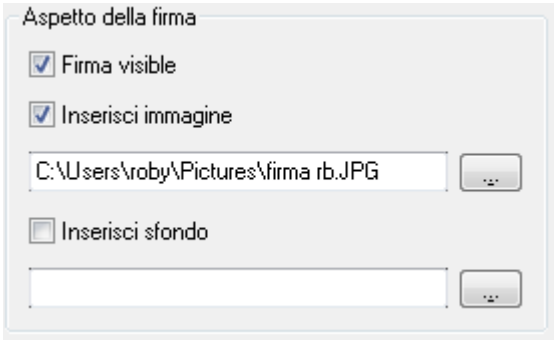


  Si veda il caso CAdES
- **Riquadro selezione e visualizzazione certificato**



Si veda il caso CAdES

- **Riquadro 'Aspetto della firma'**



Questo riquadro controlla alcuni aspetti visuali della firma, propri della modalità PAdES:

- Firma visibile – deselezionando questa casella la firma non avrà una parte visibile nel documento, sarà ispezionabile solo a livello di attributi del documento
- Inserisci immagine – l'utente può indicare un file di tipo immagine da impiegare per il rettangolo della firma; di solito si usa una scansione della propria firma autografa.
  Per esempio, la firma potrebbe apparire così:

Gentile utente,
questo file è stato firmato digitalmente con DigitalSign, il software più completo e sicuro per la firma digitale a norma di legge.
Grazie per aver scelto CompEd e DigitalSign.
Cordiali saluti,

- Inserisci sfondo – selezionando questa casella ed indicando un ulteriore file immagine si può aggiungere ad esempio un rettangolo colorato oppure una sorta di timbro.
  Ad esempio:

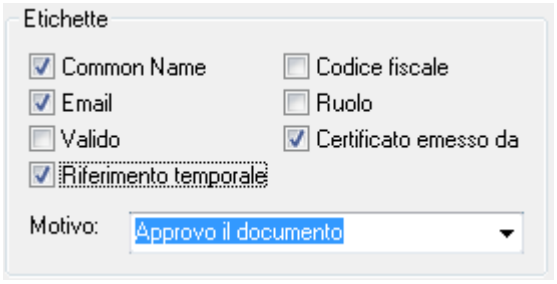
Gentile utente,

questo file è stato firmato digitalmente con DigitalSign, il software più completo e sicuro per la firma digitale a norma di legge.

Grazie per aver scelto CompEd e DigitalSign.

Cordiali saluti,

- **Riquadro 'Etichette'**

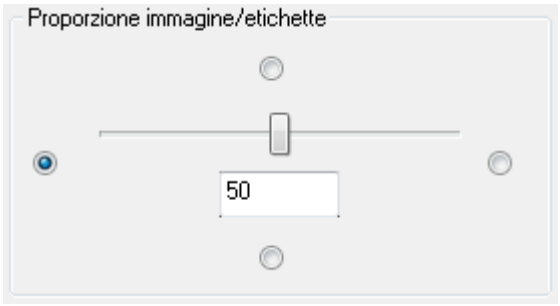


Oltre al campo "Motivo", in cui l'utente può scrivere una motivazione della firma, eventualmente selezionando tra le ultime motivazioni inserite in passato, compaiono alcune caselle selezionabili.
Ogni casella, se selezionata, provoca l'inserimento – accanto alla parte grafica della firma – di una corrispondente etichetta automaticamente impostata con i dati ricavati dal certificato.

Ad esempio, con l'impostazione esemplificata qui sopra si ottiene un risultato di questo tipo:

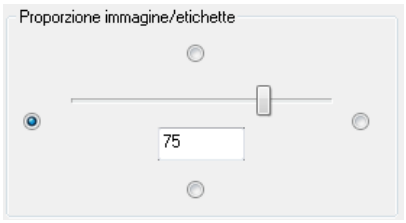
Firmato da:
ROBERTO BAUDIZZONE
Certificato emesso da: Postecom CA3, Postecom S.p.A., IT
Riferimento temporale 'SigningTime': 07-10-2014 15:54:30
Approvo il documento

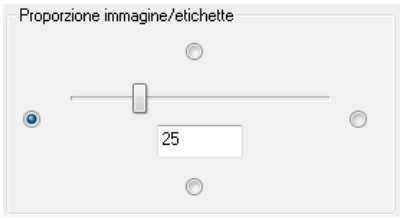
- **Proporzione Immagine/Etichette**

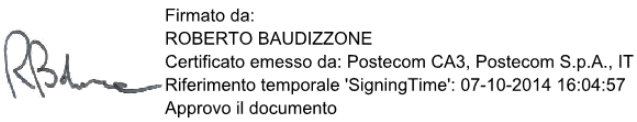


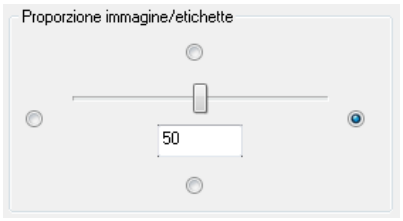
Questo controllo consente all'utente di controllare l'aspetto grafico della firma posizionando e dimensionando i due rettangoli – uno che ospita l'immagine della firma, l'altro che ospita le etichette – come desiderato.
L'impostazione qui illustrata, bottone di selezione a sinistra e proporzione al 50%, corrisponde all'immagine dell'esempio sopra.

Ecco qualche alternativa:

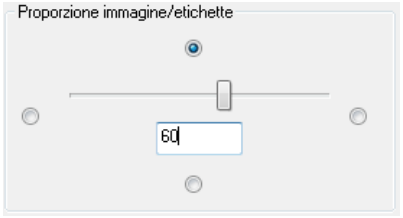





Firmato da:
ROBERTO BAUDIZZONE
Certificato emesso da: Postecom CA3, Postecom S.p.A., IT
Riferimento temporale 'SigningTime': 07-10-2014 16:04:57
Approvo il documento



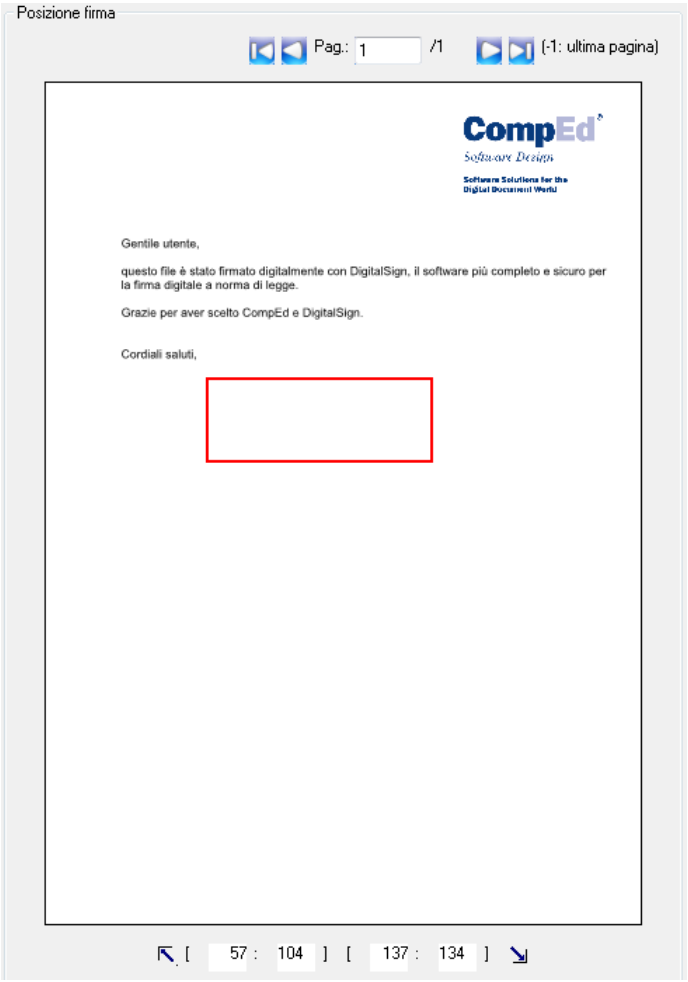
Firmato da:
ROBERTO BAUDIZZONE
Certificato emesso da: Postecom CA3, Postecom S.p.A., IT
Riferimento temporale 'SigningTime': 07-10-2014 16:07:49
Approvo il documento



Firmato da:
ROBERTO BAUDIZZONE
Certificato emesso da: Postecom CA3, Postecom S.p.A., IT
Riferimento temporale 'SigningTime': 07-10-2014 16:09:55
Approvo il documento

- **Scelta del Riferimento Temporale**
  Questa funzione opera esattamente come nel caso CAdES, a cui si rimanda

- **Posizionamento della firma**


Posizione firma
Pag.: 1 /1 (-1: ultima pagina)
CompEd
Software Design
Gentile utente,
questo file è stato firmato digitalmente con DigitalSign, il software più completo e sicuro per la firma digitale a norma di legge.
Grazie per aver scelto CompEd e DigitalSign.
Cordiali saluti,
[57 : 104] [137 : 134]

In questo riquadro l'utente definisce la posizione della firma nella pagina.
Puntando il mouse e poi spostandolo mantenendo premuto il tasto sinistro si disegna un rettangolo dal contorno rosso: tale rettangolo è l'area coperta dalla firma, intendendo sia la parte grafica che la parte etichette, secondo le proporzioni impostate.
I controlli in altro permettono di scegliere la pagina su cui posizionare la firma. Opzionalmente è possibile digitare direttamente il numero di pagina, mentre digitando il valore -1 si indica al sistema che la firma sarà posizionata nell'ultima pagina.
I 4 campi editabili alla base del riquadro rappresentano le coordinate dell'angolo superiore sinistro e di quello inferiore destro, rispettivamente.

Con il bottone

si conferma l'operazione

Con il bottone

si chiude senza generare la firma

3.5.3 Aggiungi Firma Grafometrica

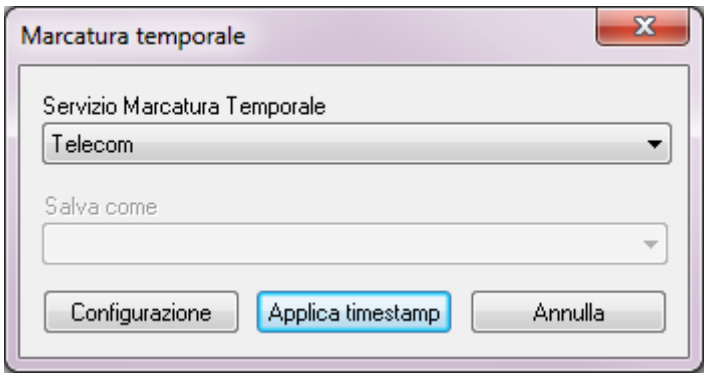
Funzione non disponibile con DigitalSign Reader

NOTA: questa funzione è abilitata solo se è installato il modulo opzionale BioSign Windows Client.

3.5.4 Marca Temporale

Funzione non disponibile con DigitalSign Reader e con DigitalSign Lite

Permette di associare una marca temporale ad un documento.
Si noti che la marca temporale è associata all'intero documento, che può essere formata o meno. É una procedura simile ma non del tutto identica all'apposizione di una marca temporale ad una singola firma, a titolo di "rifrimento temporale".

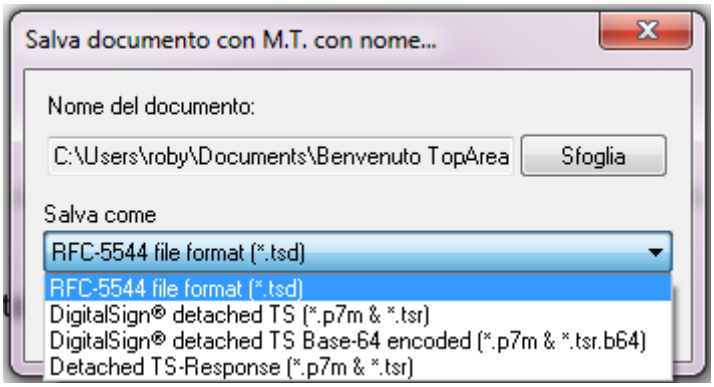


Il sistema presenta questa finestra di dialogo, per chiedere conferma all'utente.
DigitalSign può operare con diversi account di marcatura temporale, da configurare opportunamente tramite il bottone **Configurazione** (equivalente al menu **Strumenti -> Configurazione Servizi**), giungendo al modulo di configurazione specifico.

La *listbox* della finestra mostra l'account indicato come predefinito, ma consente, nel caso vi siano più account configurati, di scegliere quale impiegare.

- Il bottone **Configurazione** conduce al modulo di configurazione degli account di marcatura temporale
- Il bottone **Applica timestamp** esegue l'operazione, collegandosi al server della TSA ed ottenendo la marca temporale associata al documento su cui si sta operando
- Il bottone **Annulla** chiude l'operazione senza richiedere la marca temporale alla TSA.

Si noti che subito dopo aver eseguito l'operazione di applicazione del timestamp la marca temporale viene mantenuta solo in memoria.
Soltanto al momento in cui l'utente disporrà il salvataggio su disco (con **File -> Salva Documento** o **Salva Documento con nome…**) verrà richiesto all'utente di scegliere una modalità di rappresentazione tra quelle supportate da DigitalSign.

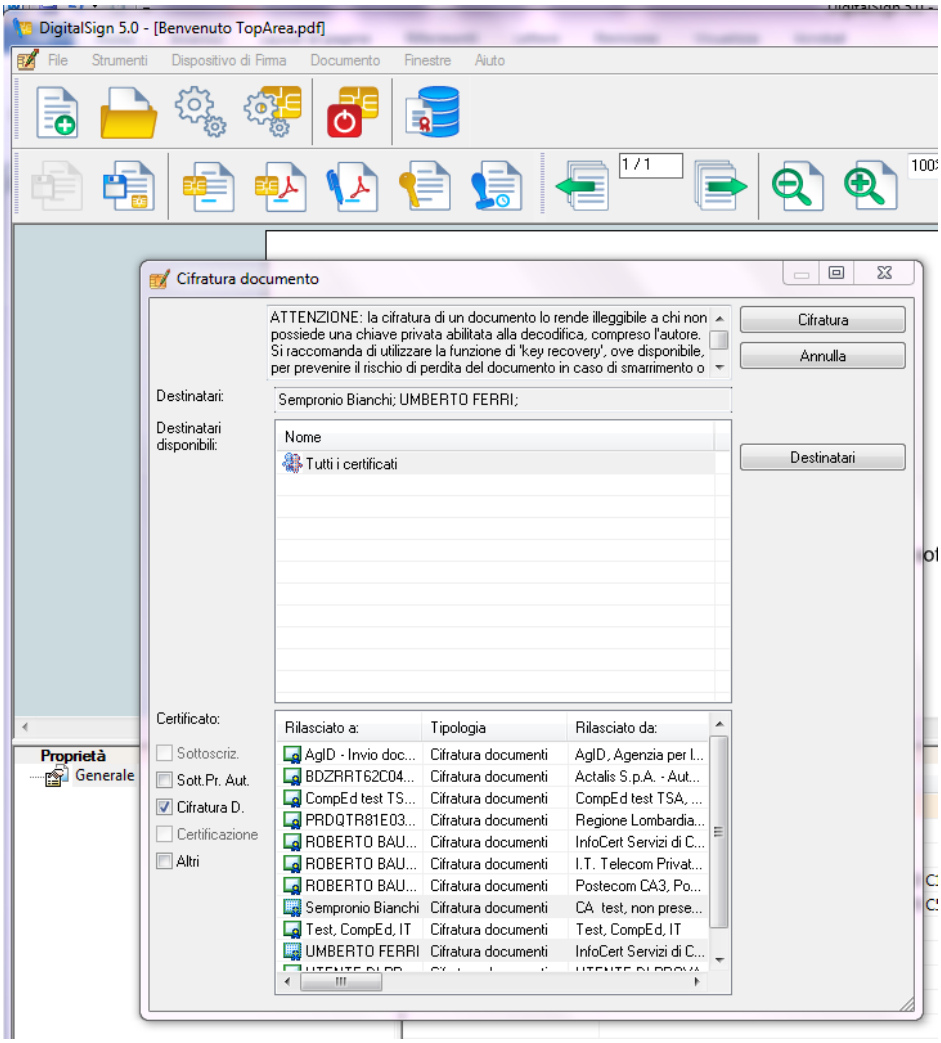

Salva documento con M.T. con nome...
Nome del documento:
C:\Users\roby\Documents\Benvenuto TopArea
Sfoglia
Salva come
RFC-5544 file format (*.tsd)
RFC-5544 file format (*.tsd)
DigitalSign® detached TS (*.p7m & *.tsr)
DigitalSign® detached TS Base-64 encoded (*.p7m & *.tsr.b64)
Detached TS-Response (*.p7m & *.tsr)

3.5.5 Destinatario Cifratura

Funzione non disponibile con DigitalSign Reader

Permette di cifrare il contenuto del documento correntemente aperto a beneficio di uno o più destinatari.
Per i dettagli sulle modalità attuate da DigitalSign per cifrare i dati si veda la sezione relativa.
Si tenga comunque presente che la cifratura attuata da DigitalSign è in prima approssimazione di tipo "asimmetrico": si cifra utilizzando la chiave pubblica del soggetto abilitato a leggere i dati, in modo che quest'ultimo possa leggerli usando la corrispondente chiave privata a sua esclusiva disposizione.
In effetti è possibile cifrare a beneficio di molteplici soggetti, che vengono definiti "destinatari".

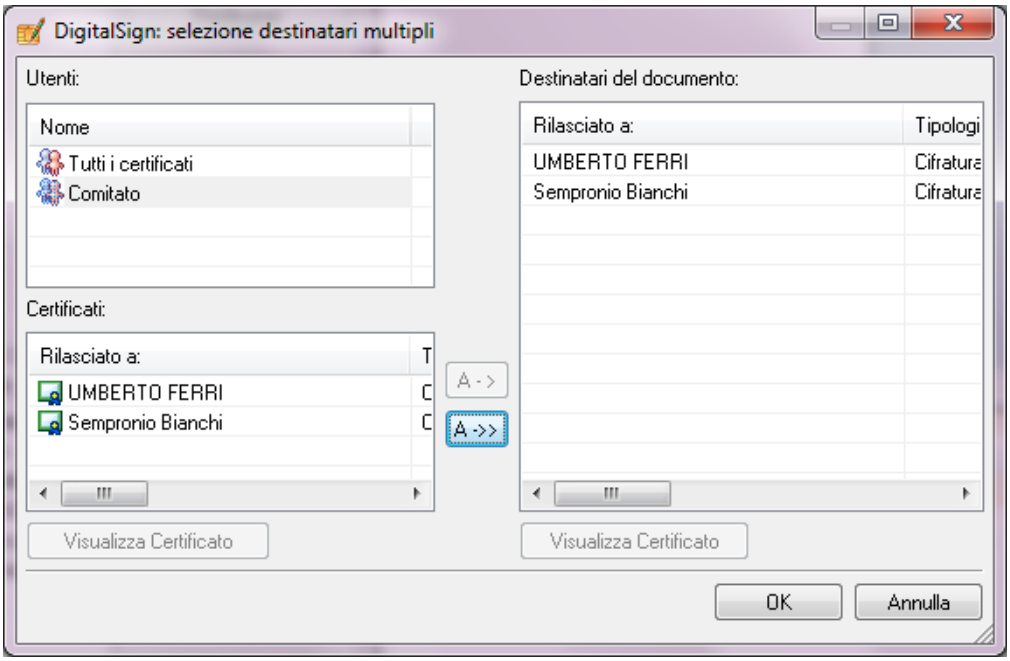
DigitalSign include sempre nella lista di questi destinatari lo stesso autore del messaggio, in modo che esso possa sempre leggere il contenuto del documento. A tale scopo DigitalSign richiede che, al momento in cui si richiede la cifratura di un documento aperto, sia inserita una smartcard, così da leggere il certificato da impiegare e da disporre della chiave privata necessaria alla rivisualizzazione una volta eseguita la codifica.
Ecco cosa appare sullo schermo appena si attiva il comando:



La schermata presenta una lista suddivisa in due riquadri, il primo dei quali mostra tutti i Gruppi di destinatari definiti (incluso il gruppo speciale **Tutti gli utenti**). Il secondo riquadro mostra tutti i certificati appartenente al Gruppo selezionato.
La definizione dei Gruppi si effettua dal modulo di gestione del DB locale dei certificati.

L'utente può posizionarsi sul riquadro inferiore e scegliere uno specifico singolo destinatario, oppure posizionarsi sul riquadro superiore e scegliere un intero Gruppo (escluso Tutti gli utenti): agendo sul bottone **Cifratura** per chiudere la finestra con la selezione effettuata.

Oppure l'utente può desiderare una selezione più articolata di destinatari, magari includendo più gruppi ed alcuni soggetti singoli, agendo sul bottone **Destinatari**, che conduce a questa schermata:



Il riquadro in alto a sinistra elenca i Gruppi disponibili; il riquadro sottostante mostra i certificati contenuti nel Gruppo selezionato.
Si opera selezionando un Gruppo nel primo riquadro oppure un destinatario singolo nel secondo riquadro, quindi premendo il bottone **[A ->]** oppure **[A ->>]** per includere il singolo destinatario o l'intero gruppo, rispettivamente, nella lista finale.
Nel riquadro di destra è sempre possibile selezionare un destinatario ed eliminarlo dalla lista con il tasto **[Canc]**.

- Con il bottone **Annulla**, naturalmente, si esce senza aggiornare la lista.
- Con i bottoni **Visualizza Certificato** è possibile ispezionare i certificati dei riquadri corrispondenti.

Dopo aver cifrato un documento l'utente può desiderare di cancellare dal proprio sistema la versione originale (non cifrata) del documento. Questo è possibile con la funzione Wipe File.

NOTA IMPORTANTE: per facilitare l'utilizzo della cifratura anche con certificati autoprodotti DigitalSign non richiede che i relativi certificati siano verificati in termini di attendibilità del Certificatore che li ha emessi.
Tuttavia l'utente dovrebbe assicurarsi dell'autenticità del certificato di un destinatario, specie se tale certificato corrisponde ad un soggetto non conosciuto personalmente o se è stato ricevuto via email.
Le funzioni di visualizzazione del certificato, in ogni contesto, consentono di effettuare la verifica.

NOTA IMPORTANTE: qualora si utilizzino le funzionalità di cifratura per rendere riservati i propri documenti si tenga sempre presente che l'apertura dei documenti cifrati richiede la disponibilità della chiave privata.
Se si utilizzano dunque chiavi contenute nelle smartcard o chiavette ottenute dai Certificatori per la firma digitale si consideri la difficoltà (o la impossibilità) di ottenere un duplicato di tali chiavi in caso di smarrimento o danneggiamento della smartcard.
Una buona strategia è munirsi di almeno due smartcard e includere sempre entrambi i propri certificati nella lista di destinatari.

3.5.6 Annulla Tutto

Questo comando, ove applicabile, consente di annullare le modifiche fin qui apportate al documento aperto, ripristinandone lo stato preesistente.

3.5.7 Wipe File

Funzione non disponibile con DigitalSign Reader

Questo comando viene abilitato solo dopo che si realizza la cifratura di un documento e dopo il salvataggio del documento cifrato risultante.

La funzione *"wipe"* consiste nella cancellazione del file originale (in chiaro) ed avviene solo dietro esplicita conferma dell'utente.
DigitalSign, con questa funzione, non si limita a cancellare il file, ma mette in atto alcune misure volte ad aumentare la sicurezza dell'operazione, nel senso di eliminare ogni traccia del documento non cifrato dal file system dell'utente:

1. il file viene sovrascritto per tre volte con dati casuali (per eliminare tracce dei dati originali);
2. il file viene rinominato per tre volte (per eliminare tracce del nome originale);
3. il file viene impostato a lunghezza pari a zero (per rimuovere il collegamento con i settori del dico che ospitavano i dati);
4. il file viene effettivamente cancellato a livello del sistema operativo.

NOTA IMPORTANTE: quantunque le misure descritte rappresentino quanto di meglio DigitalSign possa fare per evitare che i dati in chiaro siano recuperabili dal sistema, esistono dei limiti oggettivi sull'efficacia di tali misure:

a) se il documento originale era stato predisposto con una applicazione di tipo "office", come per esempio MS Word oppure Excel, tale applicazione probabilmente manterrà – almeno durante la redazione del documento – uno o più file temporanei che potrebbero contenere tracce dei dati. Al termine dell'esecuzione, in generale, queste applicazioni cancellano i propri file temporanei con semplici comandi di cancellazione a livello del sistema operativo. DigitalSign, evidentemente, non può nulla per evitare il recupero dei dati da questi file;
b) quando il sistema operativo adotta un file system come NTFS esso ha la possibilità di spostare autonomamente i dati di un file da una parte all'altra del disco, di fatto eseguendo delle copie dei dati. In questi casi la cancellazione accurata dei dati dall'ultima copia del file nulla può contro la ricuperabilità dei dati dalle copie preesistenti

Per quanto sopra l'utente particolarmente sensibile al problema dell'eliminazione dei propri dati sensibili dopo la cifratura di un documento dovrebbe ricorrere ad altri strumenti specializzati, che provvedano alla sovrascrittura sistematica di tutti i settori del disco dichiarati "spazio libero" dal sistema operativo.

Da ultimo è appena il caso di notare che la cancellazione della copia originale di un documento cifrato va effettuata con cautela: nel caso venisse perduta la chiave privata abilitata a decifrare il documento non esisterà più alcun modo per recuperarne il contenuto.

3.5.8 Verifica alla data

Questo comando consente di impostare una data ed ora di riferimento, diversa dall'istante presente, per la verifica delle firme digitali del documento corrente.
Si rimanda per i dettagli all'apposita sezione

3.5.9 Sottomenu Modalità Visualizzazione

Questo comando conduce ad un sottomenu contenente le varie modalità di visualizzazione supportate.

Di regola la modalità selezionata è quella Automatica, che permette a DigitalSign di utilizzare automaticamente la modalità idonea a presentare il documento.
Nel menu è anche riportata in grassetto la modalità effettiva attualmente utilizzata.

Nel caso l'utente ritenesse di utilizzare una modalità diversa (per esempio quella esadecimale) può operare la propria scelta in questo menu.

3.5.10 Sottomenu Securview ASCIII/RTF

Questo sottomenu del menu Documento è disponibile quando si opera su un documento di tipo testo oppure Rich Text Format.

Le sue funzioni sono molto intuitive e comprendono:

- **Ricerca**
  Permette di ricercare una sottostringa nel testo
- **Copia**
  Previa selezione di una porzione di testo, permette di copiarla negli appunti
- **Seleziona tutto**
  Dopo l'attivazione di questa funzione, con Copia si passa tutto il testo negli appunti
- **Imposta pagina**
  Apre una finestra di dialogo per impostare le opzioni di stampa
- **Anteprima di stampa**
  Apre la tipica funzione di anteprima di stampa per il documento

3.5.11 Sottomenu Securview Imaging

Questo sottomenu del menu Documento è disponibile quando si opera su un'immagine o un documento sostituito da grafica raster.

- **Modo Trascinamento**
  Il puntatore del mouse può essere usato (tenendo premuto il tasto sinistro) per spostare l'immagine nel riquadro di visualizzazione
- **Strumento Zoom – e Zoom +**
  Il puntatore del mouse può essere usato, mediante un click, per ridurre od aumentare il fattore di ingrandimento
- **Pagina indietro, Avanti, Selezionata**
  Queste funzioni sono abilitate solo se si opera su documenti in formato multipagina (es. TIFF) e permettono di navigare attraverso le pagine
- **Zoom In e Zoom Out**
  Simili agli strumenti corrispondenti, modificano immediatamente il fattore di ingrandimento
- **Selezione Fattore di Zoom**
  Permette di digitare direttamente il fattore di zoom desiderato
- **Zoom su selezione**
  Permette di selezionare liberamente un'area ristretta dell'immagine; rilasciando il tasto del mouse l'ingrandimento viene immediatamente modificato per ingrandire l'area selezionata
- **Adatta Larghezza, Altezza, Larghezza ed Altezza**
  Modifica l'ingrandimento in modo da rendere visibile tutta la larghezza, oppure tutta l'altezza, oppure tutta l'immagine
- **Ruota a Sinistra, a Destra, Capovolgi**
  Modifica l'orientamento dell'immagine visualizzata
- **Anteprima, Proprietà di pagina**
- Permette di configurare e controllare la stampa

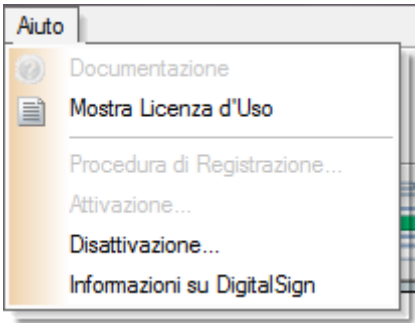
3.6 Il menu "Finestre"

Questo menu fornisce alcuni comandi standard per riorganizzare la visualizzazione delle diverse finestre controllate da DigitalSign.
Se sono aperte una o più finestre documento le ultime voci del menu corrispondono a tali finestre, consentendo di riportare in primo piano tali finestre.

3.6.1 Mostra pannelli di informazione

Attiva o disattiva la visualizzazione dei pannelli informativi decritti nella sezione dedicata

3.7 Il menu "Aiuto"



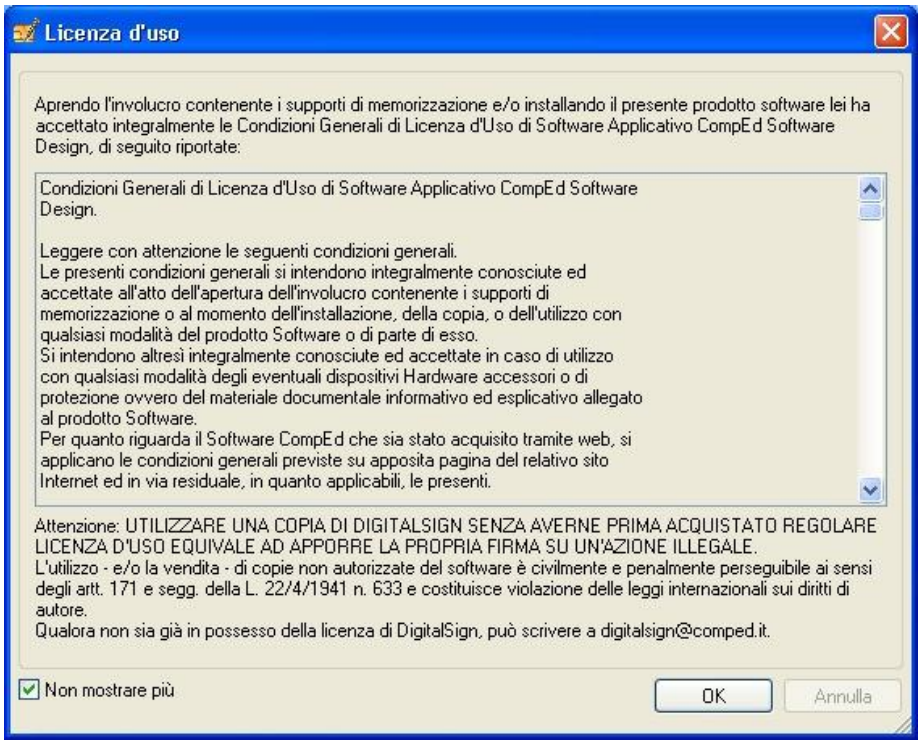
Questo menu offre alcune funzioni per visualizzare informazioni generali sulla versione del software in proprio possesso, sulla licenza d'uso, per registrare o attivare la propria copia del software.

3.7.1 Documentazione

Questa funzione provoca la visualizzazione della presente documentazione, se questa è disponibile e se la macchina dispone del software necessario alla visualizzazione (un viewer per il formato PDF).

3.7.2 Mostra Licenza d'uso

Visualizza la stessa schermata con le condizioni di licenza d'uso che viene normalmente visualizzata al primo avvio dell'applicazione.


Licenza d'uso
Aprendo l'involucro contenente i supporti di memorizzazione e/o installando il presente prodotto software lei ha accettato integralmente le Condizioni Generali di Licenza d'Uso di Software Applicativo CompEd Software Design, di seguito riportate:
Condizioni Generali di Licenza d'Uso di Software Applicativo CompEd Software Design.
Leggere con attenzione le seguenti condizioni generali.
Le presenti condizioni generali si intendono integralmente conosciute ed accettate all'atto dell'apertura dell'involucro contenente i supporti di memorizzazione o al momento dell'installazione, della copia, o dell'utilizzo con qualsiasi modalità del prodotto Software o di parte di esso.
Si intendono altresì integralmente conosciute ed accettate in caso di utilizzo con qualsiasi modalità degli eventuali dispositivi Hardware accessori o di protezione ovvero del materiale documentale informativo ed esplicativo allegato al prodotto Software.
Per quanto riguarda il Software CompEd che sia stato acquisito tramite web, si applicano le condizioni generali previste su apposita pagina del relativo sito Internet ed in via residuale, in quanto applicabili, le presenti.
Attenzione: UTILIZZARE UNA COPIA DI DIGITALSIGN SENZA AVERNE PRIMA ACQUISTATO REGOLARE LICENZA D'USO EQUIVALE AD APPORRE LA PROPRIA FIRMA SU UN'AZIONE ILLEGALE.
L'utilizzo - e/o la vendita - di copie non autorizzate del software è civilmente e penalmente perseguibile ai sensi degli artt. 171 e segg. della L. 22/4/1941 n. 633 e costituisce violazione delle leggi internazionali sui diritti di autore.
Qualora non sia già in possesso della licenza di DigitalSign, può scrivere a digitalsign@comped.it.
Non mostrare più
OK
Annulla

La schermata viene mostrata ad ogni avvio, a meno che l'utente non selezioni il checkbox **Non mostrare più**.
Questo comando nel menu **Aiuto** serve proprio a rivisualizzare il testo in questo caso ed eventualmente modificare l'istruzione di evitare le prossime visualizzazioni.

3.7.3 Procedura di Registrazione

La procedura di Registrazione è obbligatoria su alcune edizioni di DigitalSign mentre può essere opzionale in altre (Professional) o addirittura non prevista (edizioni Professional OEM).

Questo comando, se applicabile, provoca l'esecuzione della procedura di Registrazione del prodotto.
Tale procedura, per le edizioni ed i casi previsti, viene di norma eseguita automaticamente al primo avvio dell'applicazione.

3.7.4 Attivazione

La procedura di attivazione segue quella di Registrazione e consiste nell'inserimento di un Codice di Attivazione fornito dal sistema di registrazione di CompEd.
Di norma questa funzione viene eseguita automaticamente di seguito a quella di Registrazione, ma esistono alcuni casi in cui l'utente può avere la necessità di avviare la procedura autonomamente, tramite questa funzione del menu.

3.7.5 Disattivazione

Se il prodotto è stato attivato mediante un Codice di Attivazione è di norma possibile disattivarlo, recuperando il relativo Codice Licenza per una nuova installazione, su un diverso computer.

3.7.6 Informazioni su DigitalSign

Presenta una schermata di questo tipo:

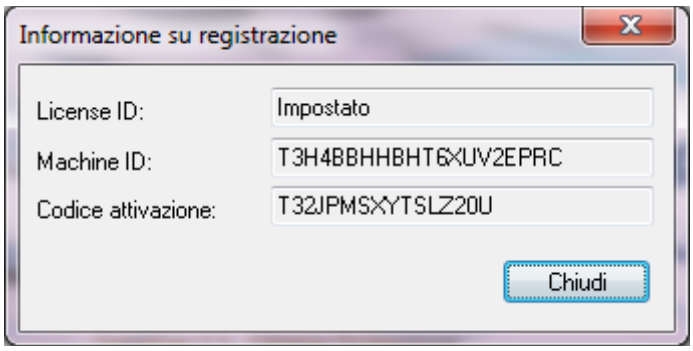
NOTA: In alcune edizioni OEM (personalizzate per grandi clienti) la visualizzazione può essere diversa e contenere il logo dell'organizzazione.

Da questa immagine l'utente può ricavare le indicazioni esatte sull'edizione e sul numero di versione della propria copia di DigitalSign, nonché sull'identità dell'utente registrato.

È anche presente un link per accedere ad una pagina di *"credits"* per **OpenSSL**: si tratta di una libreria crittografica *Open Source* il cui utilizzo (da parte di CompEd, come da parte di migliaia di operatori nel mondo) è condizionato al fatto che siano visibili da parte dell'utente le informazioni riportate a seguito dell'azionamento di tale link.

È presente anche un link alla pagina principale del sito di CompEd.

Il bottone **Info Registrazione**, se presente, apre una piccola finestra di dialogo contenente, a scopo di riferimento, le principali informazioni relative alla registrazione/attivazione del prodotto:

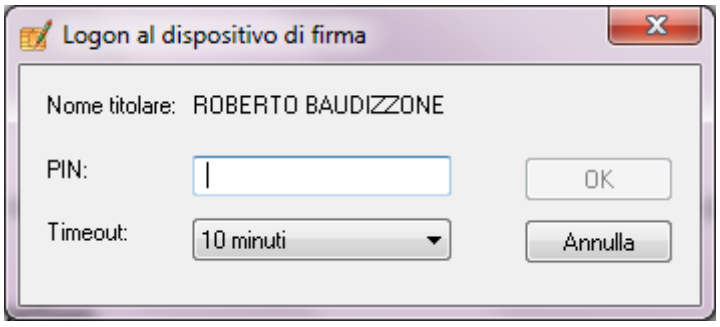


3.8 Moduli di gestione e finestre di dialogo

In questa sezione sono raccolte le descrizioni di alcuni moduli funzionali di DigitalSign utilizzati in diversi contesti.

3.8.1 Logon al dispositivo di firma

Questa finestra di dialogo viene presentata all'utente al momento in cui è richiesto che esso si identifichi – introducendo il PIN che solo il titolare deve conoscere – come legittimo titolare del dispositivo di firma correntemente in uso.



La finestra viene presentata quando l'utente richiede esplicitamente di effettuare il logon (dal menu **File**) oppure quando viene avviata un'operazione che coinvolge oggetti contenuti nell'area privata del dispositivo stesso, il quale si trova in stato di Logoff.

Nel campo **PIN** si digita appunto il codice di identificazione, che viene visualizzato in modo mascherato per impedire che venga carpito da chi osserva da dietro le spalle dell'utente.

Il campo **Timeout** corrisponde ad una *listbox* che permette di scegliere un periodo di tempo, da 1 minuto sino a 10 minuti, oppure 'nessuno'. Si tratta del tempo massimo per cui il dispositivo permane in stato di Logon senza che si verifichi alcuna attività con il dispositivo stesso.
Se si seleziona 'nessuno' il dispositivo non andrà in Logoff sino all'esplicito comando, oppure sino a che l'utente non rimuove il dispositivo o chiude l'applicazione.

- Con il bottone **OK** si conferma il dato digitato.
- Con il bottone **Annulla** si esce senza inviare il codice al dispositivo di firma.

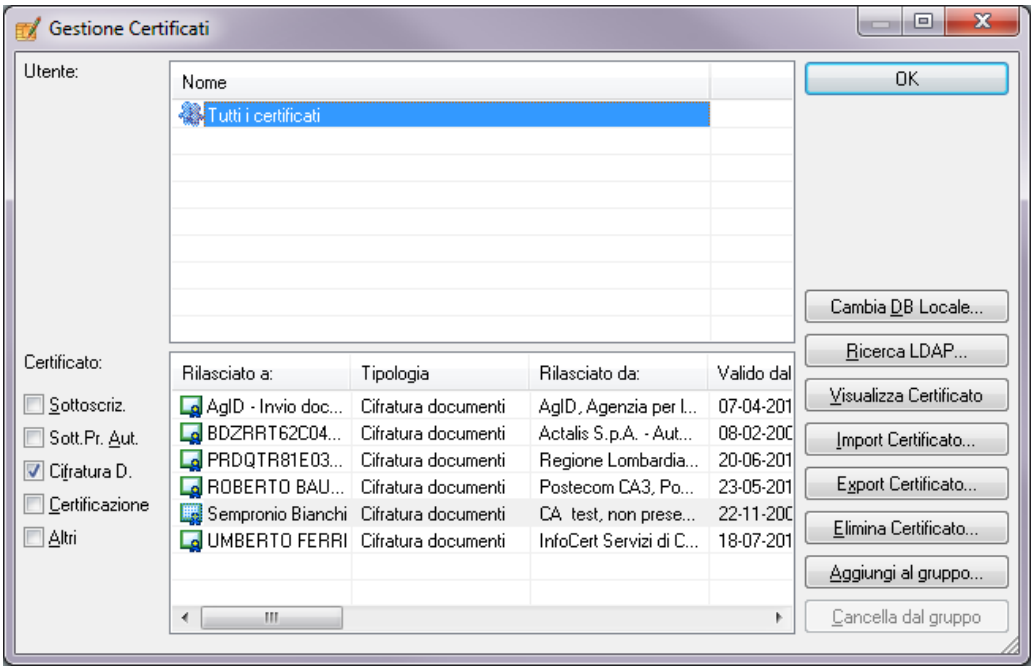
3.8.2 Modulo di gestione del DB dei Certificati

Il DB locale dei certificati è un archivio destinato, appunto, a contenere certificati.
Questo archivio può servire a diversi scopi, secondo che si operi in modalità di security **STRONG** oppure **SOFT** (si veda la sezione relativa).

- in modalità **STRONG** DigitalSign basa le verifiche dei certificati su una lista di CA dichiarate accreditate e/o attendibili tramite la firma del Presidente di CNIPA oltre che – opzionalmente – tramite la firma di un ulteriore soggetto che si assume la responsabilità di dichiarare attendibili altre CA non accreditate.
- Quindi il DB locale non serve a contenere certificati di riferimento per le operazioni di verifica, ma di fatto funge solo da "rubrica" di certificati da utilizzare per le operazioni di crittografia. Come illustrato a proposito della cifratura dei documenti, l'utente che si accinge a codificare un contenuto sceglierà da questo archivio il soggetto o i soggetti abilitati a decifrarlo;
- in modalità **SOFT** DigitalSign verifica positivamente i certificati emessi da qualunque CA il cui certificato si trovi nel DB locale, quindi il DB locale serve proprio a contenere i certificati delle CA considerate attendibili.

IL DB locale dei certificati rappresenta anche l'archivio "naturale" dei certificati emessi con la **Personal Certification Authority**.

Il modulo di gestione si presenta come nella seguente figura:



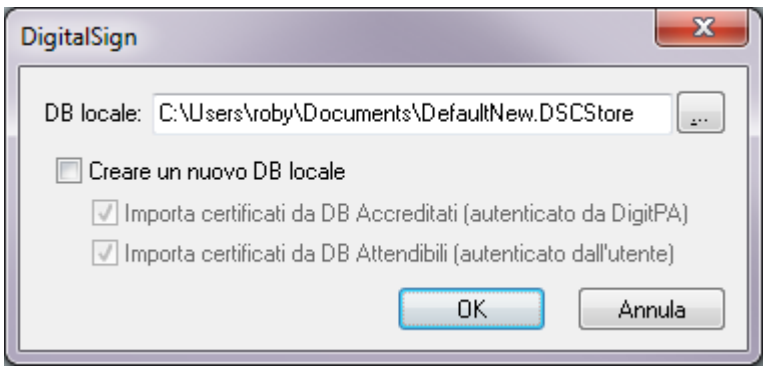
Il riquadro superiore contiene l'elenco dei **Gruppi** correntemente definiti: per default è sempre definito il gruppo speciale "Tutti gli utenti".

Il riquadro inferiore contiene una lista dei certificati contenuti nel Gruppo correntemente selezionato nella finestra superiore; se nel riquadro superiore è selezionato il Gruppo **Tutti gli utenti** allora il riquadro inferiore mostra tutti i certificati dell'archivio.

Si noti che diversi certificati rilasciati ad uno stesso soggetto da diverse Certification Authority possono scriverne il nominativo in modo differente, facendo sì che in questa finestra tale soggetto appaia come due o più soggetti diversi.

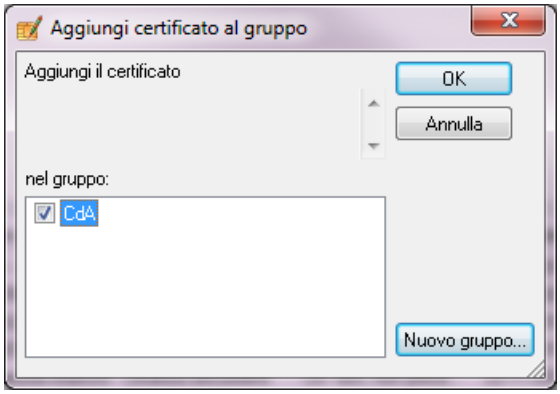
Sulla sinistra compare una batteria di *checkbox* che permette di abilitare o disabilitare la visualizzazione di diverse tipologie di certificato.

- Con il bottone **OK** si chiude la finestra
- Con il bottone **Cambia DB Locale** è possibile mettere in uso un diverso DB.
  Compare in tal caso una finestra di questo tipo:



  È possibile selezionare un diverso file, sfogliando con il bottone **[…]**, oppure crearne uno nuovo – vuoto – impostando il nome e selezionando l'apposito *checkbox*.
- Con il bottone **Ricerca LDAP** è possibile accedere al server LDAP gestito da un certificatore e ricercare certificati. La lista dei server disponibili per questa ricerca si gestisce attraverso il menu Strumenti -> Configurazione Servizi -> Elenchi in linea LDAP.
- Con **Visualizza Certificato** si apre la finestra di visualizzazione del certificato selezionato.
- Con **Import Certificato** è possibile importare nel DB un certificato disponibile su file.

- Con **Export Certificato** è possibile esportare su file il certificato correntemente selezionato
- Con **Elimina certificato** si rimuove dal DB il certificato selezionato
- Con **Aggiungi a Gruppo** è possibile includere il certificato correntemente selezionato in un particolare Gruppo, eventualmente creato appositamente.
  Scopo principale dei Gruppi è predefinire delle "liste di destinatari" da utilizzare frequentemente per le operazioni di cifratura dei contenuti.
  Si apre una ulteriore finestra di dialogo:



  La finestra mostra i Gruppi già definiti (eventualmente vuota); se il gruppo a cui si intende aggiungere il certificato selezionato è già esistente è sufficiente fare click sulla casella corrispondente. Altrimenti è possibile creare subito un Nuovo Gruppo con il bottone corrispondente.

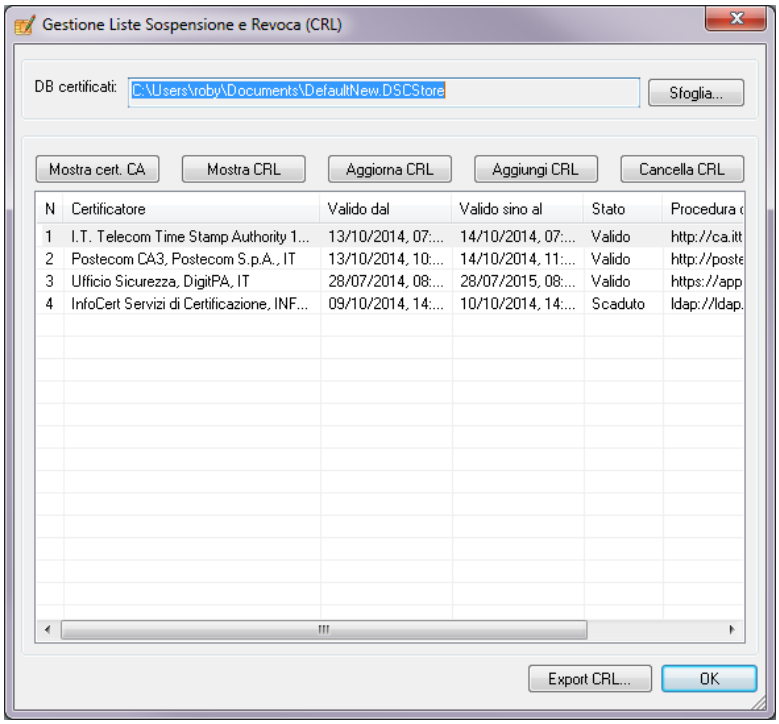
- Con **Rimuovi dal Gruppo** è possibile far sì che il certificato correntemente selezionato nel riquadro inferiore (e quindi appartenente al Gruppo selezionato nel riquadro superiore) venga eliminato dal gruppo stesso.

3.8.3 Modulo di Gestione delle Liste di Sospensione e Revoca (CRL)

Man mano che DigitalSign esegue operazioni di verifica di certificati, se è attiva la funzione di verifica dello stato di sospensione e revoca, accede ai server delle CA che hanno emesso i certificati e scarica le relative CRL (Liste di Sospensione e Revoca).
Si ricorda che l'indirizzo URL a cui si reperisce una CRL è scritto nel certificato stesso, nell'estensione standard CDP (CRL Distribution Point), protetta dalla firma del Certificatore stesso.

Ogni CRL scaricata viene automaticamente memorizzata all'interno dello stesso file che ospita anche il DB locale, sovrascrivendo l'eventuale copia più vecchia della stessa lista.

Il modulo di gestione delle CRL si presenta come in figura:



La lista presenta tutte le CRL presenti nell'archivio locale, con una organizzazione in colonne:

- **Certificatore**: il nominativo del certificatore che ha emesso la lista
- **Valido dal:** la data ed ora di inizio validità della lista. Coincide con la data ed ora di emissione da parte del certificatore
- **Valido sino al:** rappresenta il temine di validità della CRL, che dovrebbe coincidere con la pubblicazione del prossimo aggiornamento della CRL da parte del certificatore
- **Stato:** valido o non valido, in base al momento attuale ed alla finestra di validità dichiarata con i due campi "Valido dal" e "Valido sino al"

NOTA: una CRL compare nella lista solo se DigitalSign si è trovato a verificare un certificato che punta a tale lista. Il fatto poi che la copia in archivio sia "Valida" o "Scaduta" dipende dal fatto che tale verifica sia stata fatta di recente (cioè nel periodo di validità nominale) oppure più indietro nel tempo: se una CRL scade ma non serve a verificare un certificato DigitalSign non si preoccupa di aggiornarla automaticamente.

In alto compare il nome (completo di percorso) del file del DB locale certificati che contiene anche le CRL sotto osservazione. Con il bottone **Sfoglia** è possibile esplorare altri file dello stesso tipo.

- con il bottone **Mostra certificato di CA** si ottiene la visualizzazione del certificato della Certification Authority che ha emesso la CRL selezionata, tramite l'apposito viewer
- Con il bottone **Mostra CRL** si visualizza il contenuto della CRL correntemente selezionata, mediante un viewer specifico
- Con il bottone **Aggiorna CRL** si provoca l'immediata rilettura della CRL aggiornata dal server della CA. Si noti che questa funzione non è utilizzabile con tutte le CA: può funzionare solo nel caso in cui il certificato della CA contenga l'estensione CDP (CRL Distribution Point) e che alla URL così ottenuta sia presente la CRL corrispondente
- Con **Aggiungi CRL** è possibile caricare nell'archivio una CRL disponibile su un file, ottenuta con altri mezzi
- Con **Cancella CRL** si può eliminare dall'archivio la CRL selezionata.
- Con **Export CRL** è possibile esportare su un file la CRL selezionata
- Con il bottone **OK** si chiude la finestra

Per informazioni sulle strategie attuate da DigitalSign nell'utilizzo delle CRL per la verifica di firme e certificati si veda la sezione relativa.

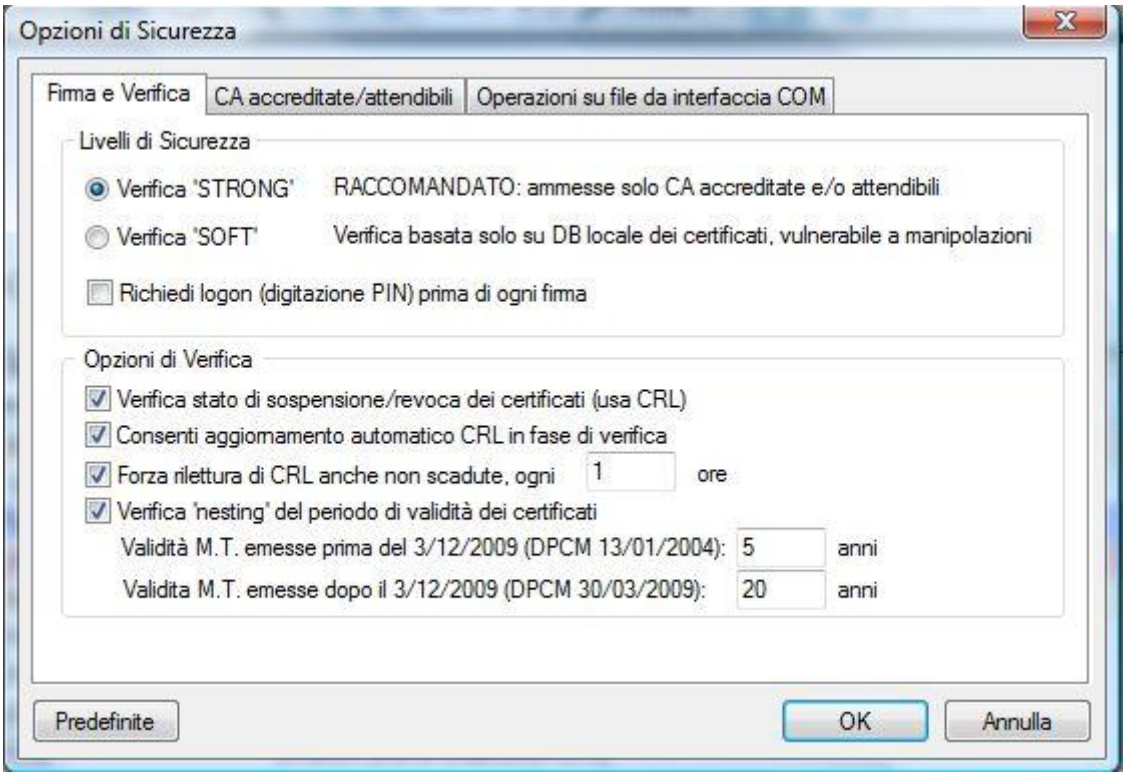
3.8.4 Modulo di Gestione delle Opzioni di Security

Questo modulo di configurazione presenta tre diverse cartelle per gestire altrettante serie di parametri.

Per tutte le cartelle sono disponibili i seguenti bottoni:

- **Predefinite** – ripristina i valori di default
- **OK** – salva le modifiche e chiude la finestra
- **Annulla** – chiude la finestra senza salvare le modifiche eventualmente apportate

3.8.4.1 Firma e verifica


Opzioni di Sicurezza
Firma e Verifica
CA accreditate/attendibili
Operazioni su file da interfaccia COM
Livelli di Sicurezza
Verifica 'STRONG'
RACCOMANDATO: ammesse solo CA accreditate e/o attendibili
Verifica 'SOFT'
Verifica basata solo su DB locale dei certificati, vulnerabile a manipolazioni
Richiedi logon (digitazione PIN) prima di ogni firma
Opzioni di Verifica
Verifica stato di sospensione/revoca dei certificati (usa CRL)
Consenti aggiornamento automatico CRL in fase di verifica
Forza rilettura di CRL anche non scadute, ogni 1 ore
Verifica 'nesting' del periodo di validità dei certificati
Validità M.T. emesse prima del 3/12/2009 (DPCM 13/01/2004): 5 anni
Validita M.T. emesse dopo il 3/12/2009 (DPCM 30/03/2009): 20 anni
Predefinite
OK
Annulla

Questo pannello consente di configurare la strategia di verifica ed il comportamento di DigitalSign in fase di firma.

Il riquadro superiore permette di scegliere, per mezzo di una coppia di *radio button*, tra la modalità di verifica **STRONG** e la modalità **SOFT**.

- in modalità **STRONG** DigitalSign considera attendibili soltanto i certificati emessi da una CA inclusa nella *'trust list'*.
  La trust list è un elenco di certificati di CA costituito da:
  - l'elenco ufficiale delle CA accreditate (TSL) pubblicato da AgID
  - l'elenco ufficiale delle CA che emettono certificati CNS, anch'esso di fonte AgID
  - l'elenco firmato di ulteriori CA attendibili (opzionale, si veda la prossima sezione)
  - i certificati di CA eventualmente contenuti nella smartcard inserita

  NOTA: in fase di verifica di un certificato o di una firma DigitalSign mostra esplicitamente in quale di questi sottoinsiemi ha trovato il certificato della CA pertinente.

- In modalità **SOFT** DigitalSign considera attendibili i certificati emessi da qualunque CA il cui certificato sia presente nel DB locale dei certificati. Questa modalità è comoda per test ed esperimenti, ma non dovrebbe essere usata in contesti di utilizzo effettivo.

Il riquadro sottostante presenta una serie di *checkbox* che controllano il comportamento in fase di verifica:

- **Verifica dello stato di sospensione/revoca dei certificati** – se attivo istruisce DigitalSign a verificare i certificati anche in merito all'eventuale stato di sospensione o revoca, tramite la relativa CRL (Lista di Sospensione o Revoca). Se questa opzione non è attiva DigitalSign mostra sempre un apposito messaggio di *warning* in occasione di ogni verifica.

- **Consenti aggiornamento automatico della CRL in fase di verifica** – se attivo consente a DigitalSign, in occasione della verifica di un certificato, di scaricare automaticamente la relativa CRL nel caso non disponga di una copia sufficientemente aggiornata.
  Se questa opzione non è attiva DigitalSign chiede conferma prima di operare lo scaricamento.
  La CRL viene in ogni caso prelevata dall'indirizzo codificato all'interno del certificato (CRL Distribution Point) e protetto dalla firma della CA.
  Naturalmente le CRL possono essere scaricate ed utilizzate solo se si dispone di un collegamento ad Internet.

- **Forza rilettura di CRL anche non scadute, ogni <*x*> ore** – ogni CRL viene pubblicata dalla CA corredata di informazioni sul periodo di validità (più esattamente sull'istante pianificato per il prossimo aggiornamento). Per le CA accreditate in Italia il periodo di validità varia da alcune ore sino a 24 ore; la normale strategia di verifica è quella di considerare valida una CRL per tutto il tempo di validità dichiarata: se si verificano più certificati emessi dalla stessa CA, in generale solo la prima verifica provocherà l'effettivo scaricamento della CRL, dopo di che si continua ad utilizzare la copia scaricata localmente.
  Attivando questo *checkbox*, tuttavia, si istruisce DigitalSign ad anticipare il nuovo scaricamento della CRL trascorso un certo tempo dall'ultima volta in cui la lista era stata effettivamente scaricata, anche se essa è ancora nominalmente valida. Questo accorgimento consente di beneficiare con la massima tempestività di eventuali pubblicazioni anticipate da parte dei Certificatori.

- **Verifica "nesting" del periodo di validità dei certificati** - questa opzione consente di attivare o disattivare una funzione di verifica soggetta a diverse interpretazioni da parte di diversi addetti ai lavori, che cerchiamo di spiegare.
  Si ricordi che un certificato intestato ad un soggetto è sempre emesso da un Certificatore, il quale lo firma utilizzando la propria chiave privata associata al proprio certificato di CA.
  Certa letteratura tecnica prescrive che in nessun caso un certificatore possa emettere un certificato il cui periodo di validità superi il periodo di validità del certificato di CA usato per firmarlo (ciò appare ragionevole, perché quando il certificato di CA sarà scaduto il certificato in questione sarebbe ancora valido, ma la verifica non potrà comunque essere complessivamente superata a causa della non validità del certificato di CA). Questo concetto è chiamato *nesting* del periodo di validità (l'intervallo di validità del certificato emesso è totalmente compreso - *nested* - nell'intervallo di validità dell'emittente).
  Tuttavia non si tratta di una regola imposta dagli standard, quanto di un vincolo implementato nei sistemi più autorevoli e diffusi: alcuni certificatori non osservano (o almeno non osservavano) questa regola mettendo in circolazione certificati la cui validità sconfina dai limiti di validità del certificato di CA.
  Tornando alla configurazione di DigitalSign, se si attiva questa opzione i certificati che violano il principio del *nesting* non saranno considerati validi, altrimenti il problema verrà ignorato (fintanto che sarà ancora valido il certificato di CA relativo!).

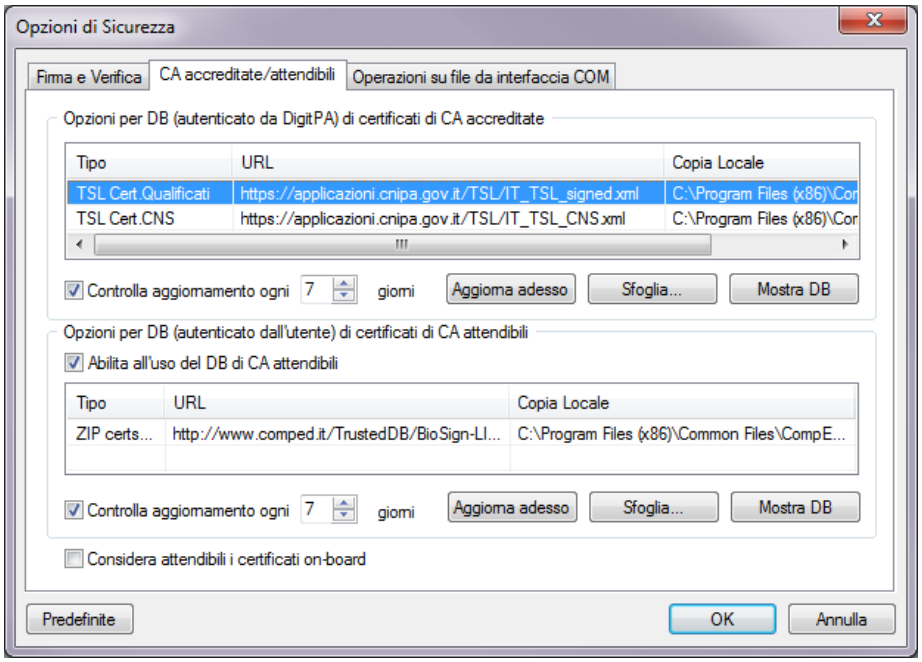
Seguono poi due parametri connessi con il periodo di validità legale delle Marche Temporali:

- **Validità Marche Temporali emesse prima del 3/12/2009 (ex DPCM 13/01/2004) <*x*> anni**
  Il DPCM 13/01/2004, all'art. 50, obbligava i certificatori a conservare copia di tutte le marche temporali emesse per un periodo minimo di 5 anni, oppure più a lungo a seguito di accordi con i clienti. Lo stesso decreto chiariva poi che i documenti firmati digitalmente e corredati di una marca temporale – ovviamente corrispondente ad un istante di tempo in cui la firma fosse realmente valida – mantenessero la proria validità anche dopo la scadenza del certificato usato per la sottoscrizione.
  Questo parametro consente di impostare il periodo di validità per le marche temporali in esame (per default 5 anni)
- **Validità Marche Temporali emesse dopo il 3/12/2009 (ex DPCM 30/03/2009) <*y*> anni**
  Il DPCM 30/03/2009, all'art. 49, modifica l'obbligo estendendolo a 20, ferma restando la facoltà di accordi certificatore-cliente per tempi di conservazione più lunghi.
  Questo parametro consente di impostare la durata di default pari a 20 anni o periodi ancora più lunghi.

La data del 3/12/2009 è quella di entrata in vigore dell'obbligo di conservazione per 20 anni stabilito dal DPCM 30/3/2009.
Quindi i parametri descritti servono a DigitalSign per decidere sulla durata effettiva della validità di una marca temporale rispetto all'emissione.

Se una marca temporale era stata emessa oltre 5 anni prima del 3/12/2009 allora il 3 Dicembre 2009 probabilmente la sua copia nell'archivio del certificatore non esiste più, dunque il documento non ha più il pieno valore probatorio.
Ma se la marca fosse stata emessa, per esempio, il 10 dicembre 2004 allora il 3 dicembre 2009 la copia d'archivio esisteva ancora e quindi l'obbligo di conservazione si estende ad un totale di 20 anni; e quindi, per i successivi 15 anni, il documento è ancora valido.

3.8.4.2 CA accreditate/attendibili



Questo pannello controlla i punti di riferimento utilizzati da DigitalSign per considerare attendibili i certificati sottoposti a verifica in modalità **STRONG**.

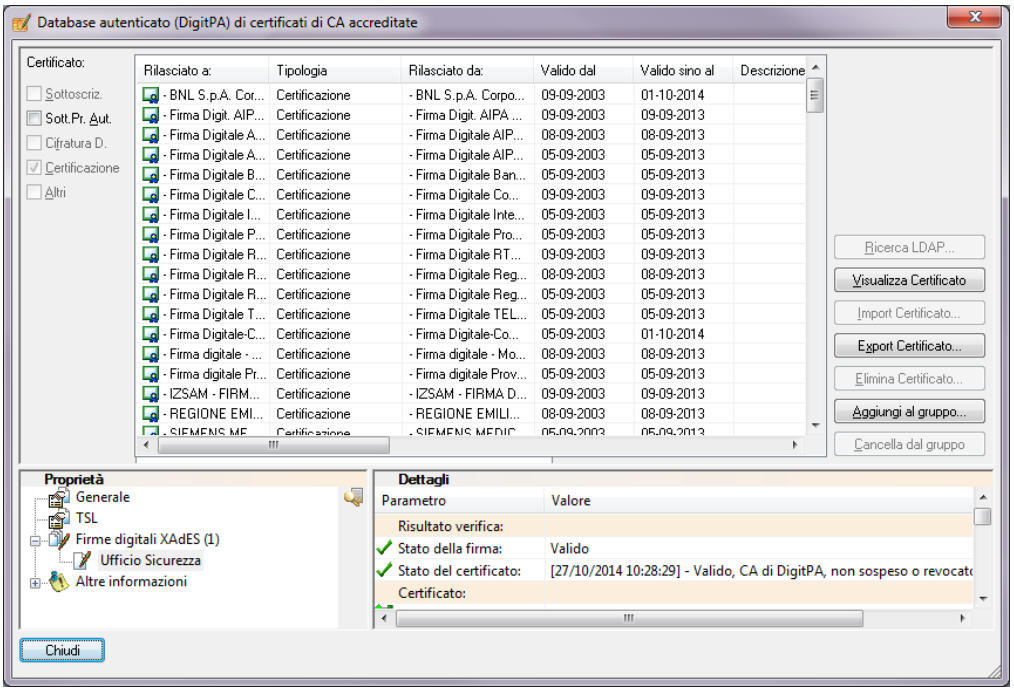
Il riquadro superiore – **Opzioni per le tabelle autenticate AgID per la verifica dei Certificati Qualificati e CNS** – riguarda la fonte principale, sempre in uso in modalità **STRONG**.
L'Agenzia per l'Italia Digitale mantiene appunto due elenchi ufficiali, uno contenente i certificati delle CA accreditate per l'emissione di Certificati Qualificati, l'altro contenente i certificati delle CA autorizzate all'emissione di certificati CNS.

Tali elenchi sono pubblicati in formato standard TSL, protetti con una firma digitale e disponibili ad indirizzi Internet ufficiali.

La tabella in alto mostra i due elenchi, i tipi di file di riferimento, la URL di scaricamento (*read-only*, perché non deve essere possibile leggere un elenco diverso da quello ufficiale), il percorso locale su cui il file viene memorizzato.

I controlli sottostanti hanno le seguenti funzioni:

- Il checkbox **Controlla aggiornamento ogni <x> giorni** permette di impostare un aggiornamento automatico, con la periodicità desiderata
- Il bottone **Aggiorna adesso** consente di operare un aggiornamento manuale immediato dell'elenco selezionato
- Il bottone **Sfoglia** permette di modificare il percorso della copia locale di ciascun elenco
- Il bottone **Mostra DB** visualizza il contenuto dell'elenco correntemente selezionato:



Il riquadro sottostante – **Opzioni per DB (autenticato dall'utente) di certificati di CA attendibili** – consente di estendere l'insieme delle CA considerate attendibili, oltre a quelle accreditate da CNIPA.
Lo scopo di questo elenco aggiuntivo, che può essere messo in uso o meno per mezzo del *checkbox* **Abilita all'uso del DB di CA attendibili**, può essere:

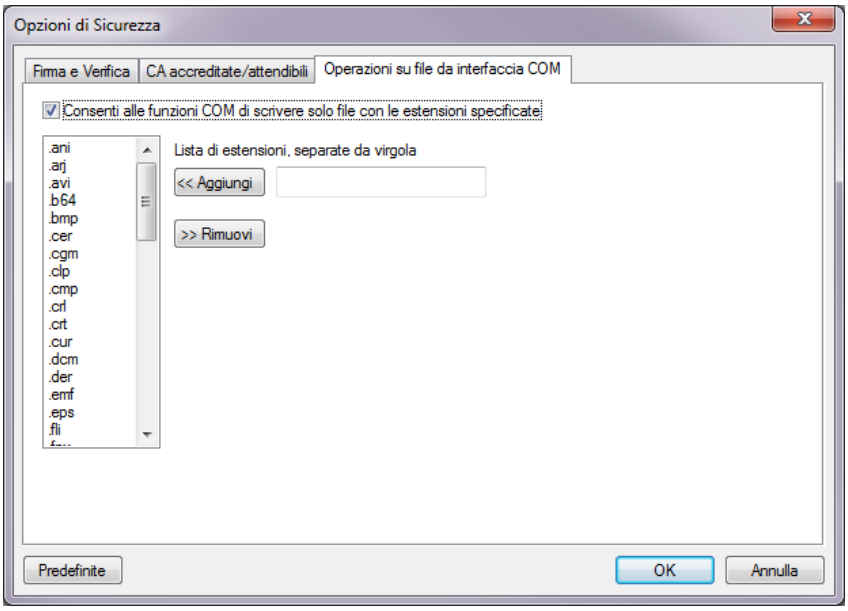
- permettere all'utente, arbitrariamente, di considerare attendibili delle CA sperimentali o comunque estranee al circuito dell'accreditamento AgID
- consentire ad una organizzazione di considerare attendibili CA distinte da quelle accreditate (per esempio quelle che emettono certificati per l'Autenticazione, l'Attestazione o la Cifratura) usufruendo degli stessi livelli di sicurezza che DigitalSign adotta per le CA accreditate

L'utente – o il responsabile dell'organizzazione – predispone un elenco di certificati di CA da considerare attendibili e lo firma digitalmente con un Certificato Qualificato. Una volta pubblicato o distribuito tale file, configurato DigitalSign ad utilizzarlo, sarà possibile verificare positivamente i certificati emessi dalle CA incluse in questo elenco. Si noti però che DigitalSign riferirà con precisione che il certificato è considerato attendibile sulla base della firma del sottoscrittore dell'archivio autenticato.

I comandi di questo riquadro funzionano esattamente come quelli del riquadro superiore, salvo che anche l'indirizzo di download è modificabile.

Infine, in fondo alla finestra, il *checkbox* **Considera attendibili i certificati on-board**, se attivato, consente di verificare positivamente i certificati emessi da una CA il cui certificato si trova nella smartcard inserita.

3.8.4.3 Operazioni su file da interfaccia COM



DigitalSign, come è noto, dispone di un'interfaccia (COM) tramite la quale altre applicazioni possono utilizzare i servizi di firma digitale, marcatura temporale, ecc. allo scopo di realizzare sistemi integrati.
Tuttavia le funzioni di questa interfaccia potrebbero essere utilizzate per introdurre nel sistema file eseguibili dannosi, come virus, trojans, e così via.
Questa finestra di dialogo consente di limitare la libertà di azione delle applicazioni client restringendo la loro possibilità di scrivere file.
Per attivare questa opzione di filtro occorre attivare il checkbox e cancellare/inserire le estensioni che si intende autorizzare.

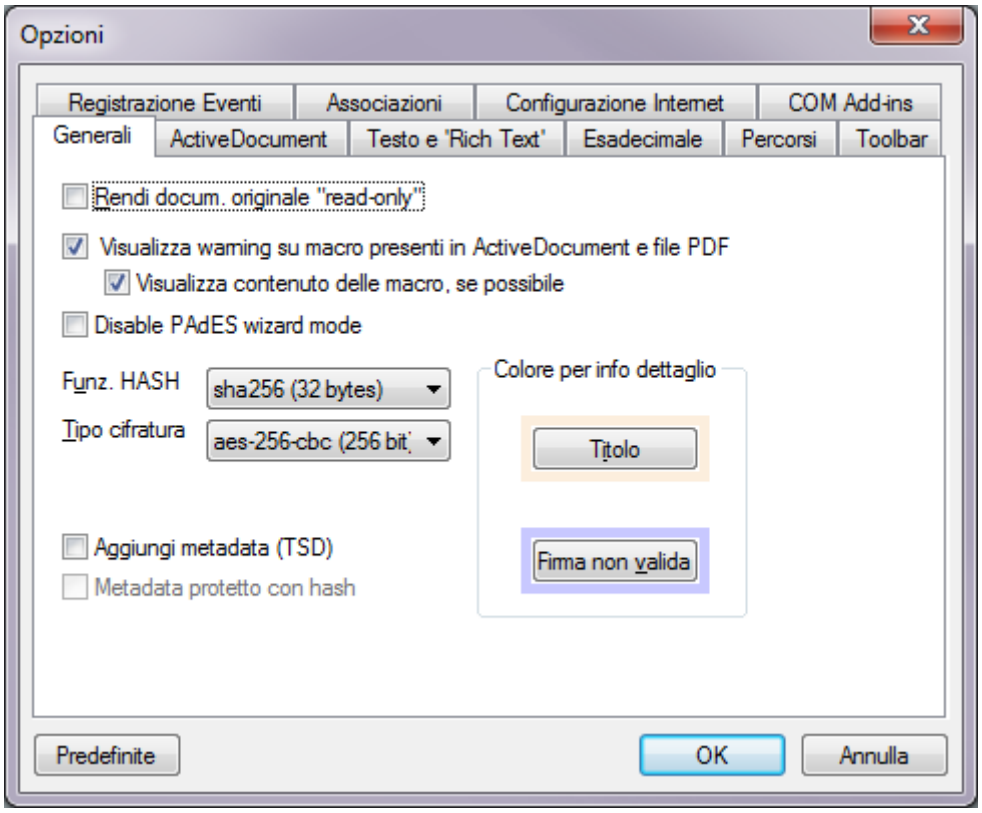
3.8.5 Modulo di Gestione delle Opzioni

Questo modulo di configurazione presenta diverse cartelle per gestire altrettante serie di parametri.
Per tutte le cartelle sono disponibili i seguenti bottoni:

- **Predefinite** – ripristina i valori di default
- **OK** – salva le modifiche e chiude la finestra
- **Annulla** – chiude la finestra senza salvare le modifiche eventualmente apportate

3.8.5.1 Generali

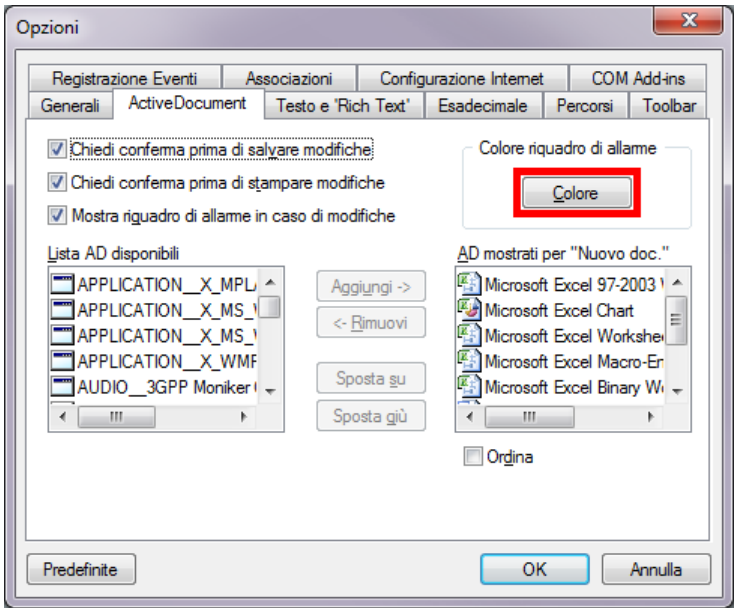
Questa finestra di dialogo consente il controllo di alcuni parametri generali.



- **Rendi documento originale *read-only*** - se questo *checkbox* è attivato, i file corrispondenti ai documenti aperti da DigitalSign non verranno modificati da eventuali operazioni compiute nell'ambito della finestra documento associata (aggiunta o rimozione di firme digitali, di marche temporali, di destinatari di cifratura, ecc.). Occorrerà usare il comando del menu **File -> Salva documento con nome...**
- **Visualizza *warning* su macro presenti in doc. ActiveDocument e PDF -** se questo *checkbox* è attivo DigitalSign mostrerà, nel pannello dei dettagli della finestra documento, una riga di informazione sul rischio o sull'effettiva presenza di elementi variabili nel documento.
- **Visualizza contenuto delle macro, se possibile** - se questo *checkbox* è attivo (ed è attivo anche quello del punto precedente), nel caso il documento sia in un formato che DigitalSign è in grado di analizzare, il pannello dettagli della finestra documento mostrerà una lista esplicita delle macro rilevate.
- **Disabilita modulo Wizard** – questo checkbox consente di disabilitare l'avvio automatico del modulo Wizard se il documento PDF caricato contiene un riferimento ad una procedura.
- **Scelta funzione HASH** – Questo controllo allo stato attuale consente unicamente di impostare la funzione hash SHA256, l'unica idonea alle Firma Qualificate.
- **Scelta del tipo da cifratura** - per default mostra l'algoritmo aes-256-cbc a 256 bit, ossia una crittografia molto fote; è possibile scegliere altri algoritmi di crittografia del contenuto del documento. Si veda anche la sezione relativa alle modalità di cifratura.
- **Colore per informazioni dettaglio** - l'utente può controllare con questo bottone il colore in cui DigitalSign visualizza nell'area PKCS#7 della finestra documento i campi di informazione relativi a firme digitali la cui verifica non viene superata positivamente.
- **Aggiungi metadati RFC5544 –** quando si appone una marca temporale a un documento già completo, si possono usare diverse modalità: mantenere documento e marca separati (modalità "detached") oppure riunirli in un unico file mediante lo standard RFC5544 (documento in formato **.tsd**). Nel secondo caso lo standard permette di includere alcuni metadati e di considerarli nel calcolo dell'impronta su cui effettuare la marcatura temporale. Scegliendo questa opzione, tuttavia, non sarà possibile convertire il documento all'altra modalità. Rinunciando ai metadati sarà possibile salvare il documento .tsd anche nel formato detached.

3.8.5.2 ActiveDocument

Questa finestra consente di controllare alcuni parametri relativi al comportamento di DigitalSign nella manipolazione di documenti aperti in una finestra documento tramite un viewer di tipo **ActiveDocument**.



Tre *checkbox* controllano il comportamento in presenza di modifiche apportate durante l'editing:

- **Chiedi conferma prima di salvare modifiche**
- **Chiedi conferma prima di stampare modifiche** – riguarda l'esecuzione di stampe di documenti modificati dopo l'apertura
- **Mostra riquadro di allarme in caso di modifiche** – se questo checkbox è attivo, in caso il documento venga modificato in fase di editing evidentemente le firme digitali preesistenti non saranno più valide; un riquadro lampeggiante di allarme informerà l'utente di questa circostanza. Un bottone **colore riquadro allarme** permette di configurare il "look" del riquadro di allarme di cui al punto precedente.

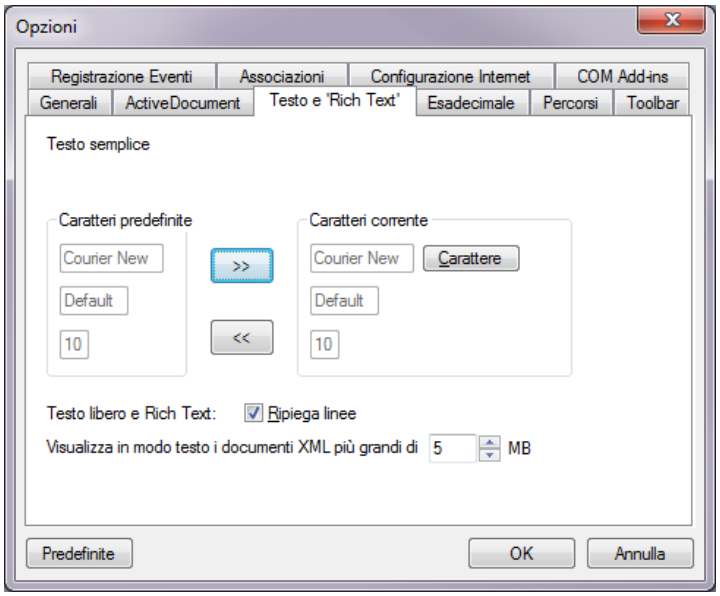
Nella parte bassa della finestra compaiono due riquadri tramite i quali è possibile configurare il sistema su quali applicazioni compatibili ActiveDocument, tra quelle installate nel sistema, sia possibile usare con DigitalSign.
Il riquadro di sinistra mostra tutte le applicazioni ActiveDocument ancora disponibili, quello di destra mostra quali applicazioni sono già state abilitate all'uso come viewer ActiveDocument per DigitalSign.

- Il bottone **Aggiungi** provoca il passaggio dell'applicazione correntemente selezionata nel riquadro di sinistra verso quello di destra (ossia inserimento tra le applicazioni abilitate)
- Il bottone **Rimuovi** provoca il passaggio dell'applicazione correntemente selezionata nel riquadro di sinistra verso quello di destra (ossia rimozione dalle applicazioni abilitate).
- Il bottone **Sposta su** provoca lo spostamento di una posizione verso l'alto dell'applicazione correntemente selezionata nel riquadro di destra.
- Il bottone **Sposta giù** provoca lo spostamento di una posizione verso il basso dell'applicazione correntemente selezionata nel riquadro di destra.

NOTA: la prima applicazione della lista del riquadro di destra è quella scelta per default quando si crea un nuovo documento.

3.8.5.3 Testo e "Rich Text"

Questa finestra di dialogo controlla alcuni parametri relativi al comportamento del viewer per documenti di puro testo e per documenti *rich text.*

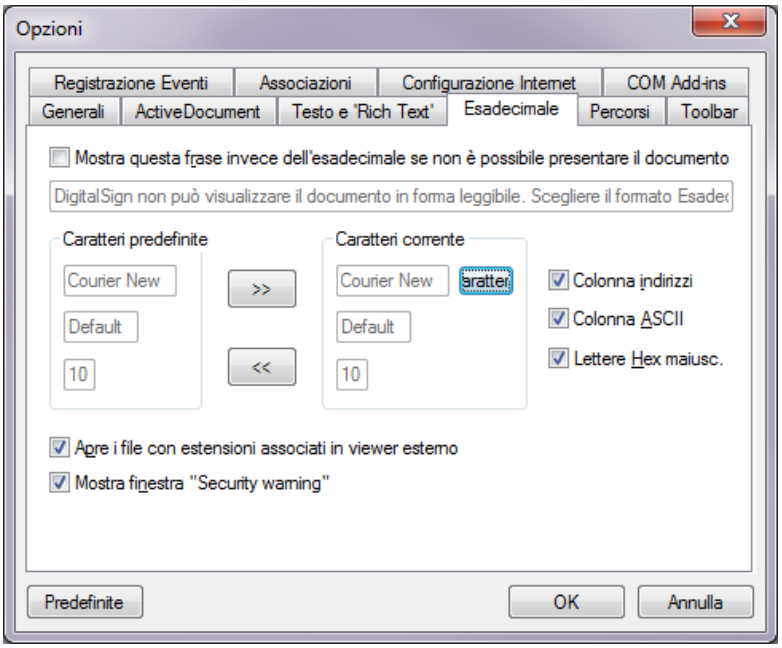


Due aree della finestra consentono di specificare un particolare font da utilizzare per la rappresentazione dei documenti di puro testo.
Il Font corrente è quello utilizzato per il documento correntemente aperto, il font di default è quello che verrà utilizzato per tutti i documenti di questo tipo.

- Tramite il bottone **[<<]** il font di default assume una configurazione identica a quella del font corrente.
- Tramite il bottone **[>>]** il font corrente viene riconfigurato in accordo con il font di default.
- Il *checkbox* **ripiega linee**, se attivo, istruisce DigitalSign a tagliare automaticamente le lunghe linee di testo che superano la larghezza della finestra e a riportarle su una linea successiva. Se il flag non è attivo l'utente dovrà agire sulla scroll-bar orizzontale per visualizzare tali linee lunghe.
- Il controllo **Visualizza in modo testo i documenti XML più grandi di *<x>* MB** serve a contrastare un limite di Internet Explorer (il viewer di default per i documenti XML) che provoca un abnorme consumo di memoria ed un conseguente progressivo decadimento delle prestazioni al crescere delle dimensioni dei documenti. Per ovviare a questo fenomeno DigitalSign limita l'uso di tale viewer ai file di dimensione contenuta, mostrando invece in formato di testo semplice quelli più grandi della soglia prefissata.

3.8.5.4 Esadecimale

Questa finestra di dialogo controlla alcuni parametri relativi al comportamento del viewer per dati binari di DigitalSign



Il *checkbox* **Mostra questa frase invece dell'esadecimale**, se attivo, fa sì che il viewer riporti semplicemente una frase informativa sull'impossibilità di manipolare il documento tramite un viewer specifico. Se il *checkbox* è disabilitato DigitalSign procede invece con la visualizzazione dei dati in formato esadecimale.
La frase specifica è impostabile dall'utente tramite l'*edit-box* sottostante.

Due riquadri sottostanti consentono di controllare il font da impiegare per la visualizzazione: Il font corrente è quello utilizzato per il documento correntemente aperto, il font di default è quello che verrà utilizzato per tutti i documenti di questo tipo.

- Tramite il bottone **[<<]** il font di default assume una configurazione identica a quella del font corrente.
- Tramite il bottone **[>>]** il font corrente viene riconfigurato in accordo con il font di default.

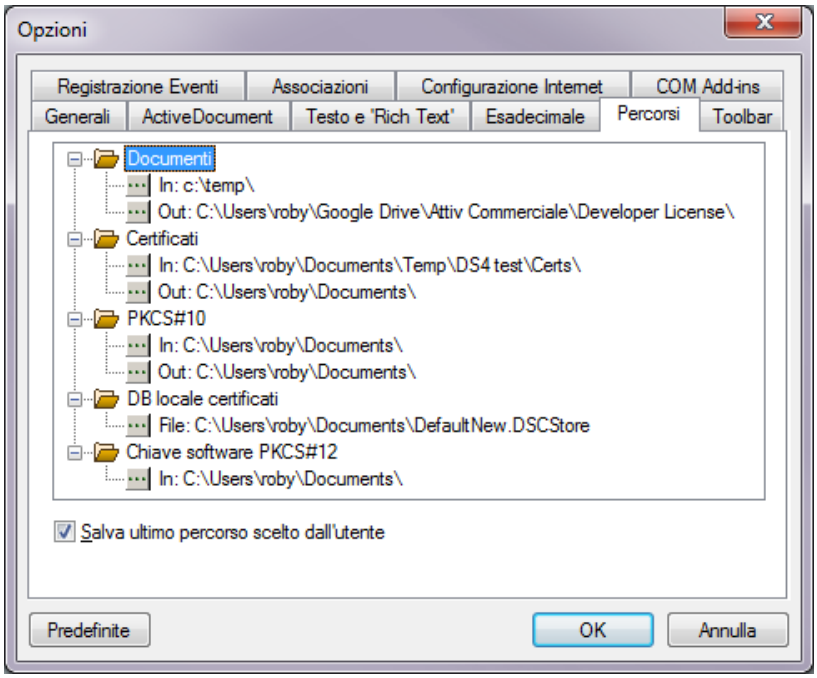
Tre *checkbox* consentono di abilitare o disabilitare individualmente la visualizzazione, rispettivamente, della **colonna degli indirizzi** (offset), della **colonna ASCII**, l'utilizzo delle **lettere maiuscole** nella presentazione dei dati esadecimali.

Il checkbox **Apri i file con estensioni associate tramite viewer esterno**, se attivo, autorizza DigitalSign a utilizzare eventuali applicazioni registrate a livello di sistema per l'estensione del file in oggetto, come viewer esterno.

Il checkbox **Mostra security warning**, se attivo, istruisce DigitalSign a mostrare, prima dell'attivazione di un viewer esterno, una schermata di avvertimento sul ridotto livello di sicurezza offerto da un viewer di questo tipo.

3.8.5.5 Percorsi

Questa finestra di dialogo consente di controllare le posizioni di default in cui DigitalSign colloca i file di diverso tipo.

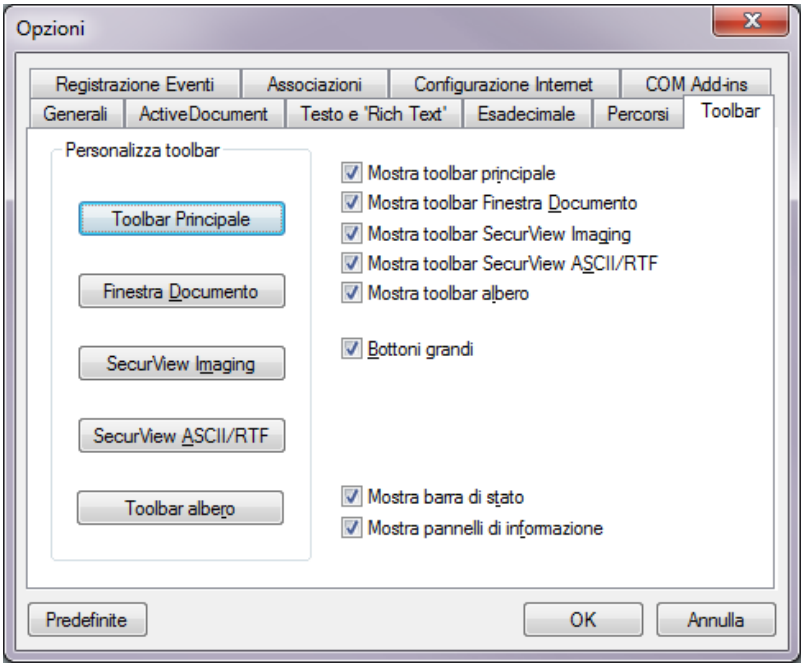


Alcuni parametri vengono aggiornati automaticamente, per esempio quando si salva un documento, ma modificando il parametro relativo di questa finestra l'utente può influire sulla proposta di default del sistema.

Il *checkbox* **Salva ultimo percorso scelto dall'utente**, se attivo, fa sì che il percorso effettivamente scelto dall'utente in una delle operazioni menzionate, venga salvato come percorso di default per le successive operazioni dello stesso tipo.

3.8.5.6 Toolbar

Questa finestra di dialogo consente di personalizzare le barre strumenti (toolbar) che DigitalSign presenta nelle diverse situazioni.



Sul lato destro della finestra sono elencati alcuni *checkbox* per controllare se DigitalSign debba o meno mostrare toolbar specifiche:

- **Mostra Toolbar principale** (quella mostrata inizialmente da DigitalSign anche quando nessuna finestra documento è aperta)

- **Mostra Finestra documento** (la toolbar specifica delle funzioni di DigitalSign mostrata all'interno di ogni finestra documento)
- **Mostra Securview Imaging** (quella associata al viewer per immagini raster)
- **Mostra Securview ASCII/RTF** (quella associata al viewer per documenti di puro testo e al viewer RTF)
- **Mostra Toolbar Albero** (quella verticale che appare sul separatore tra il pannello proprietà PKCS#7 e l'area dettagli della finestra documento)

Altri *checkbox* controllano il comportamento di DigitalSign relativamente alle toolbar:

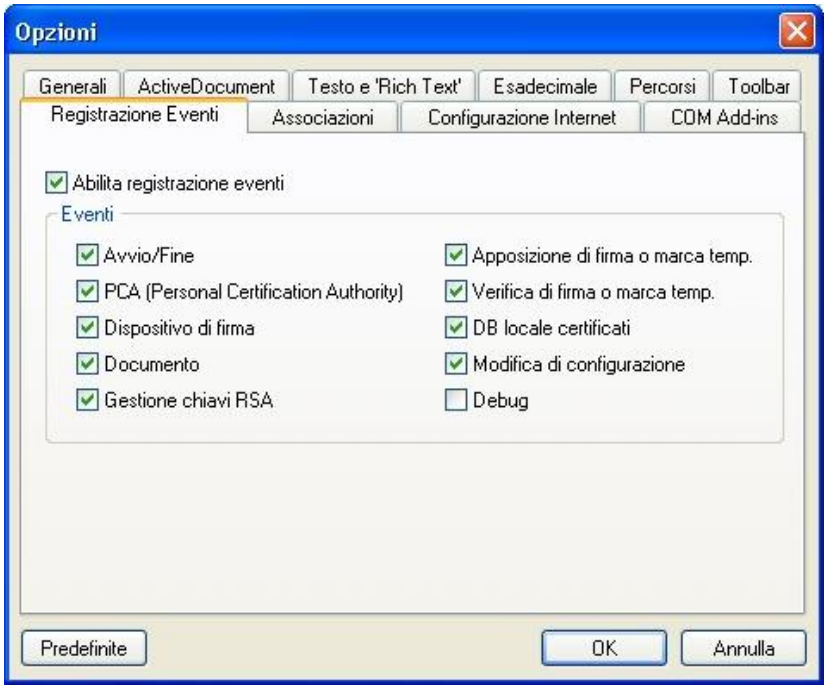
- **Bottoni grandi** - consente di controllare la dimensione dei bottoni delle toolbar
- **Mostra barra di stato** - controlla la visualizzazione della barra di stato in fondo alla finestra principale.
- **Mostra pannelli di informazione** - abilita o disabilita la visualizzazione dei pannelli informativi

Alcuni bottoni di comando permettono di personalizzare il contenuto delle diverse toolbar attraverso una specifica finestra di dialogo:

- **Toolbar principale** (quella mostrata inizialmente da DigitalSign anche quando nessuna finestra documento è aperta)
- **Finestra documento** (la toolbar specifica delle funzioni di DigitalSign mostrata all'interno di ogni finestra documento)
- **Securview Imaging** (quella associata al viewer per immagini raster)
- **Securview ASCII/RTF** (quella associata al viewer per documenti di puro testo e al viewer RTF)
- **Toolbar Albero** (quella verticale che appare sul separatore tra il pannello proprietà PKCS#7 e l'area dettagli della finestra documento)

3.8.5.7 Registrazione Eventi

Questa finestra di dialogo permette all'utente di attivare/disattivare la registrazione degli eventi e, nel caso tale funzione sia attivata, di controllare quali categorie di eventi includere nella registrazione.



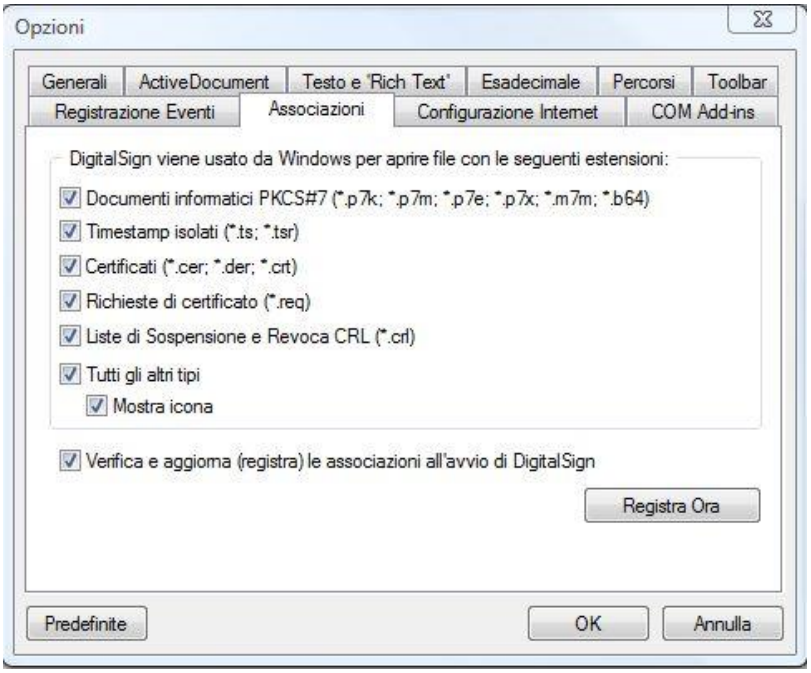
Il *checkbox* **Abilita registrazione eventi**, se attivo, fa sì che gli eventi significativi dell'attività di DigitalSign vengano effettivamente registrati.

Il riquadro sottostante, accessibile se il *checkbox* di abilitazione è attivo, consente di includere o escludere dalla registrazione le varie categorie di eventi disponibili.

NOTA: la categoria **Debug** merita particolare attenzione: se attivata provoca la scrittura di registrazioni molto dettagliate, soprattutto in materia di interfacciamento con le smartcard. L'effetto collaterale è che l'esecuzione rallenta significativamente, quindi va attivato solo in caso di necessità per analizzare situazioni problematiche.

3.8.5.8 Associazioni

Questa finestra di dialogo consente di configurare le modalità secondo cui Windows fa uso di DigitalSign per gestire i file dei tipi compatibili con DigitalSign stesso.



Il primo riquadro permette di controllare le associazioni vere e proprie di DigitalSign ai file con le diverse estensioni specifiche. Questo significa che, agendo con doppio click (da Windows) su un file appartenente ad uno dei tipi selezionati, l'apertura avverrà per default con DigitalSign.

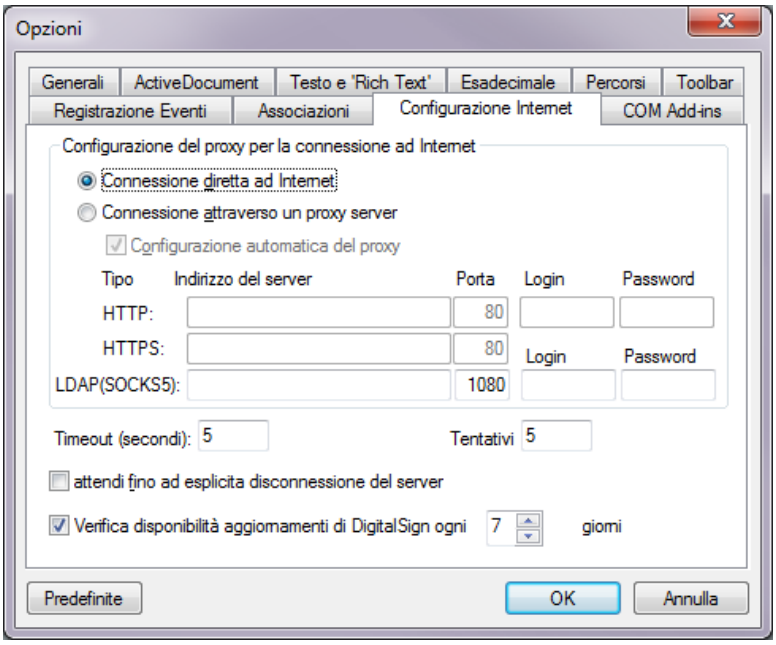
Esiste poi l'opzione **Tutti gli altri tipi**: quando questa è selezionata, se da una finestra di Windows Explorer si fa click con il tasto destro su un file di tipo generico, comparirà nel menu di apertura anche un **Apri con DigitalSign**.
Se poi è attiva anche l'opzione **Mostra icona**: il menu presenterà anche la tipica icona di DigitalSign. Se l'operazione con il tasto destro viene effettuata a livello di una cartella invece che di un singolo file, si attiverà il meccanismo firma semiautomatica di file contenuti in una cartella dalla *shell* di Windows.

Fuori dal riquadro si trova un altro checkbox, **Verifica e registra all'avvio di DigitalSign:** se questo è attivo DigitalSign riesegue ad ogni avvio la configurazione a livello di registro di sistema per tutte le associazioni qui configurate (utile nel caso in cui altre applicazioni nel frattempo avessero modificato la configurazione)

Esiste un bottone di comando specifico, **Registra ora**, che provoca la registrazione immediata in Windows della configurazione appena completata.

3.8.5.9 Configurazione Internet

Questa finestra di dialogo consente di configurare la modalità in cui DigitalSign deve accedere ad Internet, per le operazioni che lo richiedono (marcatura temporale, scaricamento degli elenchi autenticati di certificati accreditati/attendibili, consultazione delle CRL, ...).



I *radio button* del primo riquadro consentono di scegliere tra una connessione diretta (nel caso di configurazioni di rete relativamente libere) o attraverso un *proxy* aziendale.
Nel secondo caso la scelta di operare una configurazione automatica (che eredita la configurazione di Internet Explorer) risolve la gran parte delle situazioni.

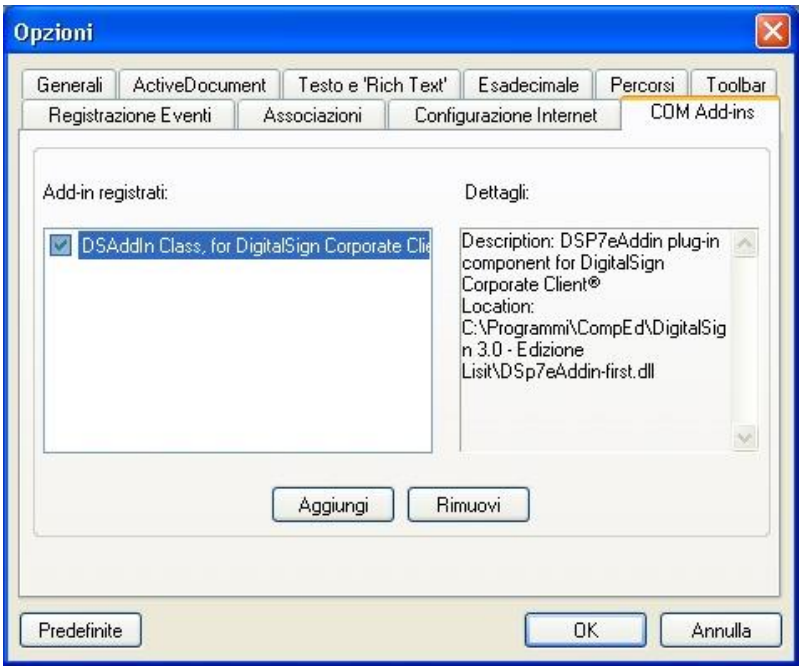
NOTA: l'eventuale configurazione del proxy ha effetto solo sulle connessioni via http e https, non sulle connessioni in LDAP.

Ove fosse necessario configurare parametri specifici, incluse le credenziali di accesso, può essere utile rivolgersi all'amministratore di sistema.

L'ultimo *checkbox* **Verifica disponibilità aggiornamenti di DigitalSign ogni <x> giorni** consente di mantenere aggiornata la propria installazione, tramite un accesso al server di CompEd.

3.8.5.10 COM Add-Ins

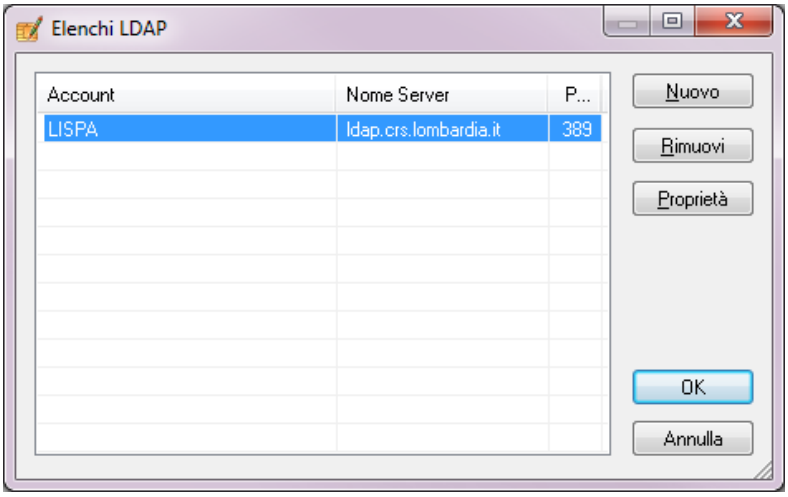
Questo pannello serve alla gestione di moduli Add-In per DigitalSign.
In generale la presenta può presentarsi vuota oppure contenere la lista degli Add-in correntemente installati:



- Con il bottone **Aggiungi** è possibile installare un nuovo Add-in (si faccia riferimento alla documentazione speciica dell'add-in che si intende installare)
- Con il bottone **Rimuovi** si opera la disinstallazione dell'add-in selezionato dalla lista

3.8.6 Modulo di Configurazione dei servizi di accesso agli elenchi di certificati LDAP

Questa finestra di dialogo consente di configurare i servizi di consultazione degli elenchi di certificati in linea.



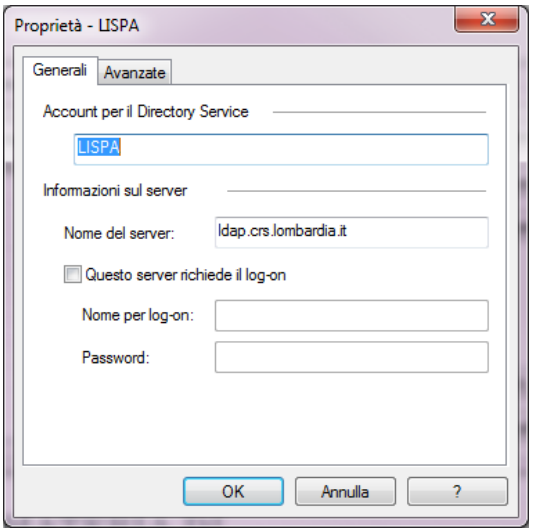
È possibile inserire diversi servizi, che corrispondono ad altrettanti server LDAP, in generale uno per ogni certificatore ritenuto di interesse.

- Il bottone **Nuovo** crea una nuova entry e conduce alla finestra di dialogo per la compilazione dei relativi parametri.
- Il bottone **Rimuovi** elimina il servizio selezionato
- Il bottone **Proprietà** conduce alla finestra di dialogo per la revisione dei parametri relativi al servizio selezionato

- Il bottone **OK** salva le modifiche apportate e chiude la finestra
- Il bottone **Annulla** chiude la finestra senza salvare le eventuali modifiche.

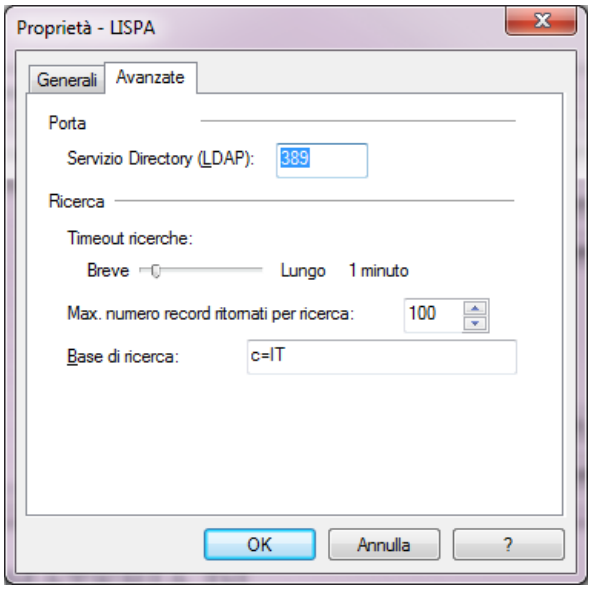
3.8.6.1 Finestra di configurazione di un servizio LDAP

Questa finestra di dialogo è in effetti organizzata in due distinte cartelle, la prima delle quali è **Generali**:



- Il **Nome Simbolico (Account)** viene attribuito dall'utente ed ha solo un significato locale, per distinguere i vari servizi attivi in DigitalSign. Tipicamente si usa il nome del certificatore che gestisce il server.
- Il **Nome del server** è in pratica l'indirizzo Internet a cui il server risponde. Questa informazione è pubblicata dal certificatore che gestisce ogni servizio
- Il *checkbox* **Questo server richiede logon** va attivato se il server in oggetto richiede che l'utente sia preventivamente registrato ed in tal caso occorre fornire anche il **nominativo** e la **password** necessari per l'accesso

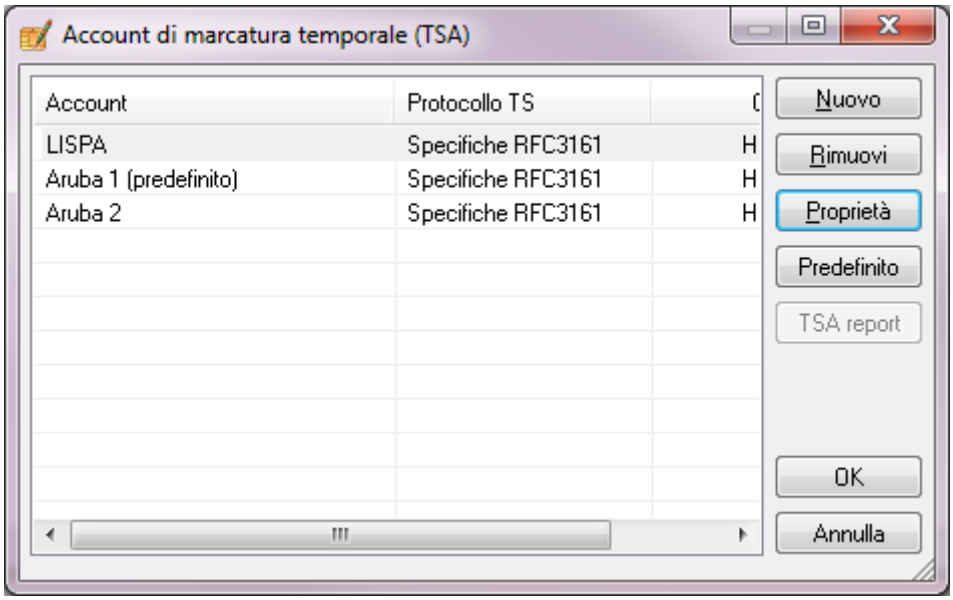
La cartella **Avanzate** si presenta come segue:



- Il **Servizio Directory** è in effetti il numero di porta, un parametro specifico del server. Il valore 389 è usato di norma da tutti i server LDAP, ma in casi particolari può essere necessario un valore diverso (consultare il gestore)
- Il **Timeout ricerche** indica il tempo massimo durante il quale DigitalSign attenderà una risposta prima di considerare la ricerca fallita. Si agisce spostando il cursore a destra o sinistra per allungare o abbreviare l'intervallo
- Il **Massimo numero record ritornati per ricerca** limita il flusso di informazioni trasferite nel caso si introduca una chiave di ricerca troppo ampia, soddisfatta da molti record. Da notare che molti server limitano comunque il numero di record ritornati
- La **Base di Ricerca** è una stringa usata per limitare la ricerca a record di una specifica categoria. I server gestiti dai certificatori accreditati CNIPA di norma esigono che la base di ricerca sia "**c=it**", altrimenti non ritornano alcun risultato.

3.8.7 Modulo di Configurazione dei servizi di Marcatura Temporale

Questo modulo permette di visualizzare, aggiungere od eliminare gli account di marcatura temporale utilizzabili.
DigitalSign consente di interagire con diversi *provider* di servizi di marcatura temporale, l'utente deve creare e configurare un *account* per ogni fornitore che intende utilizzare.
La schermata mostrata in figura visualizza tutti gli account correntemente configurati:



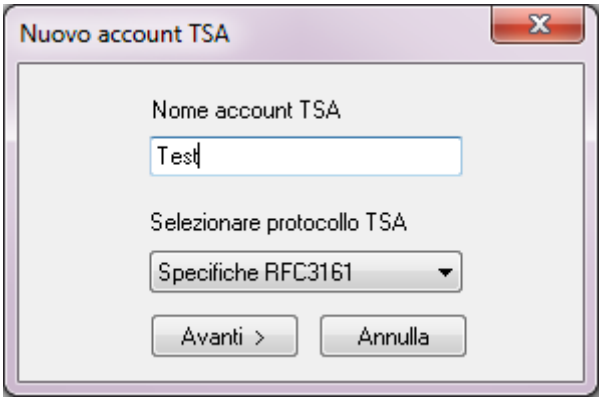
- Con il bottone **Nuovo** si passa all'inserimento di un nuovo account, per mezzo di una ulteriore finestra di dialogo
- Con il bottone **Rimuovi** è possibile eliminare l'account selezionato
- Il bottone **Proprietà** mostra le caratteristiche dell'account selezionato, con la possibilità di modificarle per mezzo di una ulteriore finestra di dialogo
- Il bottone **Predefinito** permette di indicare l'account selezionato come quello predefinito da utilizzare con tutti i comandi di marcatura temporale. Il bottone non è accessibile se l'account selezionato è già il predefinito (oppure l'unico disponibile). L'account attualmente predefinito viene indicato nella lista.
- Il bottone **TSA report** consente – per i servizi che supportano tale funzione, attualmente soltanto Infocamere – di ottenere un rapporto sul credito di marche temprale residuo

- Il bottone **OK** chiude la finestra registrando le modifiche eventualmente apportare.
- Il bottone **Annulla** chiude la finestra senza salvare le modifiche.

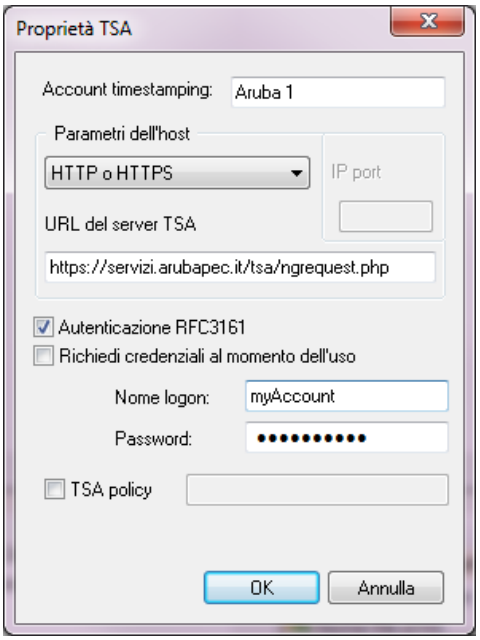
3.8.7.1 Finestra di configurazione per un account di Marcatura Temporale

Quando si richiede la creazione di un nuovo account di Marcatura Temporale occorre innanzitutto assegnare un nome all'account e scegliere il "protocollo".

Oggi tutti i certificatori devono erogare il servizio in modalità standard RFC3161, ma il sistema ancora supporta alcuni protocolli proprietari.



La schermata di configurazione per la modalità **RFC3161** si presenta come segue:



In generale si utilizzeranno i parametri di default: protocollo http o https e autenticazione RFC3161 attiva, in modo da poter fornire le credenziali di accesso.
Il resto dei parametri va ottenuto dal provider.

3.8.8 Modulo per la generazione di una CRL

Questo modulo funzionale, appartenente alla Personal Certification Authority, consente di produrre una lista di revoca da utilizzare per la verifica di certificati prodotti appunto tramite la PCA.

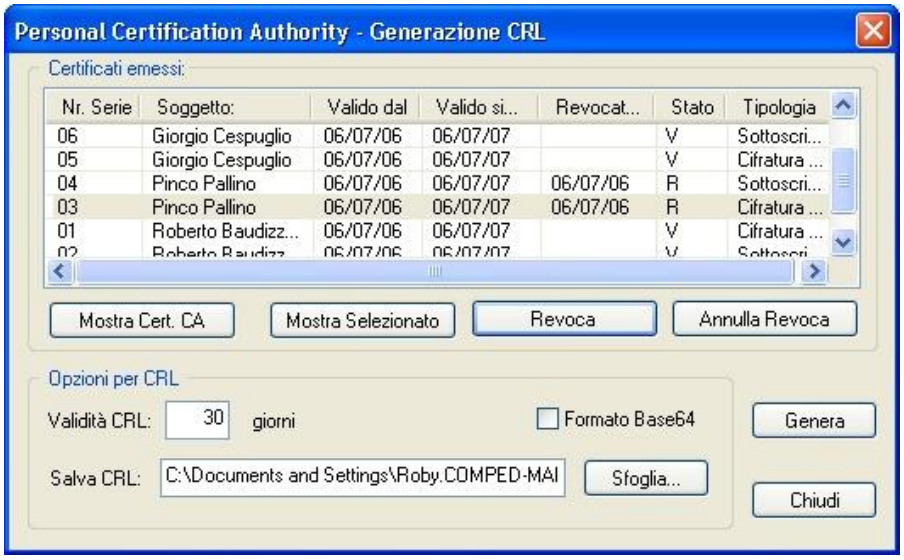
La finestra di gestione, accessibile solo se è inserita – ed in stato di logon – una smartcard contenente un certificato di CA, si presenta come in figura:

La tabella mostra tutti i certificati attualmente contenuti nel DB locale generati con il certificato di CA contenuto nel dispositivo di firma correntemente inserito.

La tabella contiene le seguenti colonne:

- numero di serie del certificato
- nominativo del titolare del certificato
- inizio validità nominale
- termine validità nominale
- data dell'eventuale sospensione/revoca
- indicatore dello stato del certificato (R=Revocato, V=Valido)

La prima volta che si accede a questo modulo la tabella mostrerà tutti i certificati in stato di validità; quando si accederà a questa funzione in seguito, dopo aver generato una lista contenente almeno un certificato in stato di revoca, la tabella continuerà a mostrare lo stato imposto in precedenza (naturalmente le informazioni vengono prelevate dall'ultima CRL caricata nel DB locale), per cui si potranno aggiornare i dati e quindi creare una nuova copia aggiornata della CRL
Si veda l'esempio corrispondente a due certificati revocati:



Alcuni bottoni comando situati sotto la tabella consentono di operare sulla tabella stessa:

- **Mostra Certificato di CA -** visualizza il certificato corrispondente alla chiave di certificazione contenuta nel dispositivo di firma per il quale si sta costruendo la CRL
- **Mostra selezionato** - mostra il certificato correntemente selezionato nella tabella
- **Revoca -** cambia lo stato del certificato selezionato
- **Annulla revoca** - ripristina lo stato di *attivo* per il certificato selezionato

Un altro riquadro consente di configurare alcune opzioni per la produzione del file che rappresenta la CRL:

- **Periodo di validità CRL <x> giorni**: tale termine viene registrato all'interno della CRL, così che in fase di consultazione sia possibile verificare se la lista è ancora attuale oppure se è obsoleta
- **Salva CRL**: l'utente deve dichiarare un nome per il file completo di percorso, eventualmente utilizzando il bottone **Sfoglia**
- **Formato Base64**: attivando questo checkbox la lista verrà esportata in tale formato

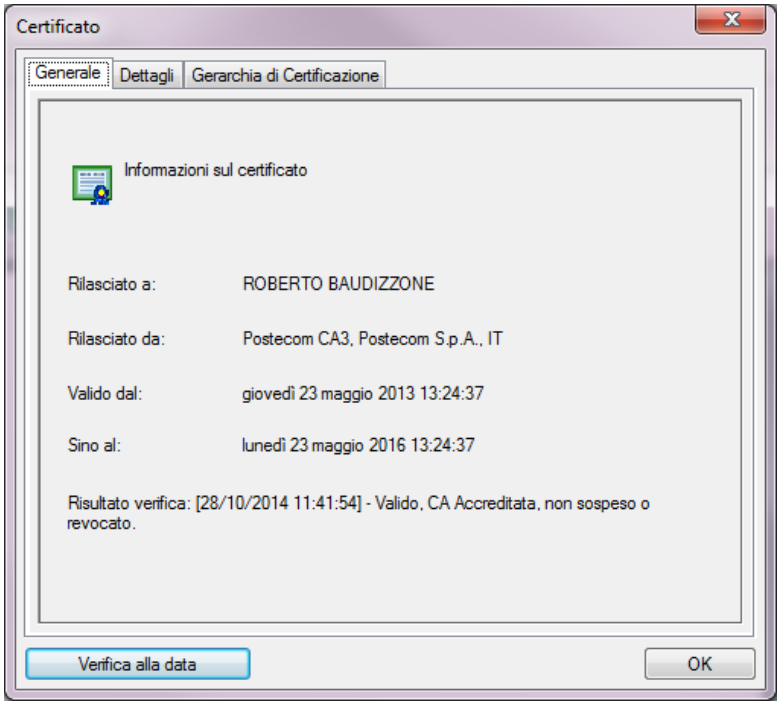
Il bottone **Genera** provoca la creazione della CRL, che conterrà i riferimenti a tutti i certificati che nella tabella riportano lo stato di revocato o sospeso. La lista verrà anche caricata nel database locale dei certificati, dal quale potrà poi essere gestita mediante l'apposito modulo di gestione.

Si noti che per mettere in esercizio la CRL prodotta è necessario che essa venga poi resa accessibile alla URL scritta in tutti i certificati prodotti dalla CA in questione, cioè quello che si trova esplicitato nel file .INI, si vedano i dettagli a proposito della Personal Certification Authority.
Naturalmente è necessario ripetere questa operazione prima di ogni scadenza della validità della CRL, evitando che gli utenti trovino alla URL predefinita una CRL scaduta.

3.8.9 Modulo di visualizzazione di un Certificato

Questo viewer viene utilizzato per presentare il contenuto di un certificato o di una richiesta di certificato. Nel caso del certificato, in generale, la visualizzazione è organizzata in tre distinte cartelle:

Generale

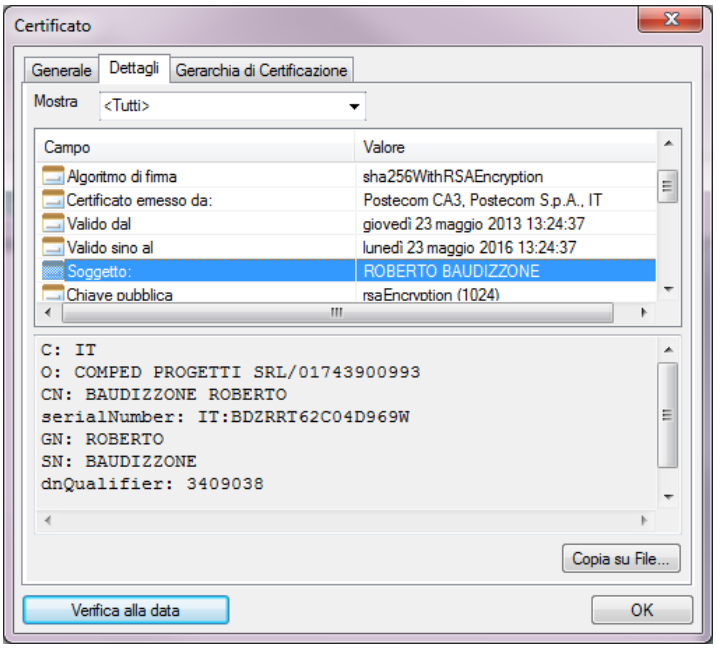

Certificato
Generale
Dettagli
Gerarchia di Certificazione
Informazioni sul certificato
Rilasciato a: ROBERTO BAUDIZZONE
Rilasciato da: Postecom CA3, Postecom S.p.A., IT
Valido dal: giovedì 23 maggio 2013 13:24:37
Sino al: lunedì 23 maggio 2016 13:24:37
Risultato verifica: [28/10/2014 11:41:54] - Valido, CA Accreditata, non sospeso o revocato.
Verifica alla data
OK

Le informazioni mostrate in questa finestra sono:

- **Rilasciato a -** il titolare del certificato e quindi della relativa coppia di chiavi
- **Rilasciato da -** il fornitore di servizi di certificazione che lo ha rilasciato (eventualmente un organo interno all'organizzazione, qualora si operi mediante la Personal Certification Authority)
- **Valido dal -** l'inizio del periodo di validità, imposto dall'autorità di certificazione
- **Sino al -** termine del periodo di validità, imposto dall'autorità di certificazione
- **Verifica certificato -** lo stato di validità del certificato, in termini di verifica della relativa firma. Il caso più normale, come quello in figura, riporta la verifica superata positivamente, il fatto che il certificato in esame è stato emesso da una CA accreditata (presso CNIPA), il fatto che non è sottoposto a revoca o sospensione.

Il bottone **Verifica alla data** consente di effettuare la verifica rispetto ad una data specifica, per verificare se il certificato era valido o meno (rispetto a scadenza o revoca).

Dettagli



La finestra presenta in alto un campo con etichetta **Mostra** che permette di scegliere se la visualizzazione deve riguardare tutte le informazioni (per default) oppure le sole "proprietà".
Il riquadro sottostante contiene una tabella di entry, ciascuna delle quali rappresenta un campo del certificato ed il relativo valore. Poiché alcuni valori (per esempio la chiave pubblica) sono troppo grandi per essere contenuti nella colonna destra della tabella, la finestra contiene un ulteriore riquadro nel quale vengono riportate per esteso le informazioni contenute nel campo del certificato correntemente selezionato.

I campi principali sono:

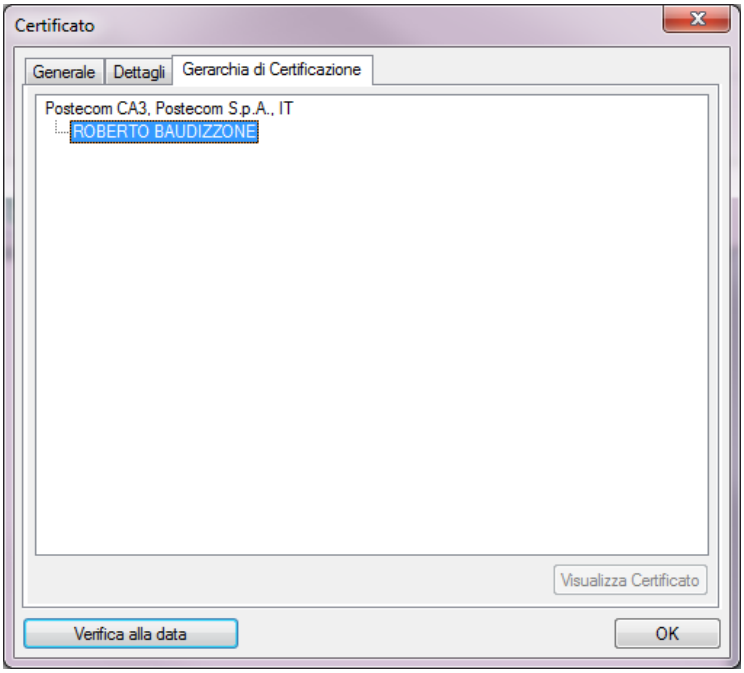
- **Versione -** numero di versione del file che contiene il certificato
- **Num. di serie -** un numero di serie univoco assegnato al certificato da parte della Certification Authority che lo ha generato. È espresso in notazione esadecimale.
- **Algoritmo di firma -** la specifica dell'algoritmo standard impiegato per la firma digitale che sigilla il certificato
- **Emesso da –** La Certification Authority le informazioni sul soggetto che ha emesso il certificato
- **Valido dal -** la specifica dell'inizio del periodo di validità del certificato
- **Valido sino al -** la specifica del termine del periodo di validità del certificato
- **Soggetto** - le informazioni sul soggetto titolare del certificato
- **Chiave pubblica** - il contenuto effettivo della chiave pubblica oggetto del certificato, espressa in notazione esadecimale
- **Algoritmo di impronta** - la specifica della funzione hash impiegata per calcolare l'impronta su cui è stata poi calcolata la firma digitale del certificato
- **Impronta** - il contenuto effettivo dell'impronta del certificato, espresso in notazione esadecimale.

In generale in certificato contiene poi altri elementi di informazioni, soprattutto se si tratta di un certificato generato in accordo con la normativa Italiana sulla firma digitale (si veda la Deliberazione CNIPA 4/2005).
Tra tali elementi di informazione si segnalano in particolare:

- **X509v3 Key Usage** – ossia la specifica sulla tipologia della chiave riferita dal certificato stesso. I certificati per la firma digitale “forte” in Italia devono avere unicamente il valore “Non repudiation” in questo campo.
- **X509v3 CRL Distribution Points** – è l’indirizzo Internet a cui si trova la lista dei certificati sospesi e revocati pubblicata dalla CA che ha emesso questo certificato.

Il bottone **Copia su file** permette di esportare il certificato su un file (.CER) in formato X.509 (DER encoded) scelto dall'utente.

Gerarchia di Certificazione



Questa schermata mostra visivamente la catena di certificazione di un certificato di chiave pubblica.

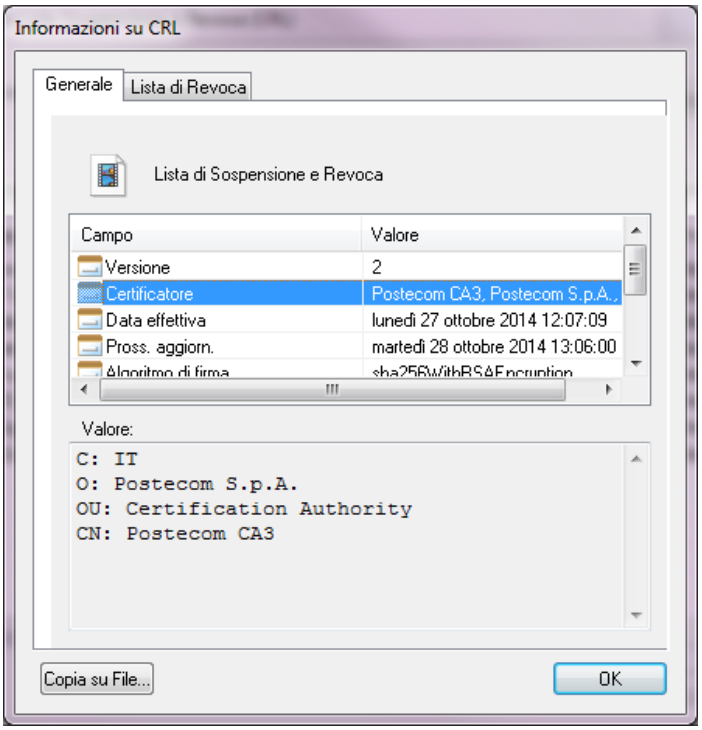
Ogni certificato deve infatti essere firmato digitalmente dalla Certification Authority che lo emette, il cui certificato deve a sua volta essere disponibile per la verifica e potrebbe a sua volta essere stato emesso da un altro soggetto di livello più elevato.
Si risale così una catena sino al raggiungimento di un certificato di livello root, firmato da se stesso.

Lo schema dell'infrastruttura italiana prevede solo due livelli, come in figura.

Selezionando il certificato del livello superiore diventa disponibile il bottone **Visualizza Certificato**, che consente di esaminare il certificato della CA emittente.

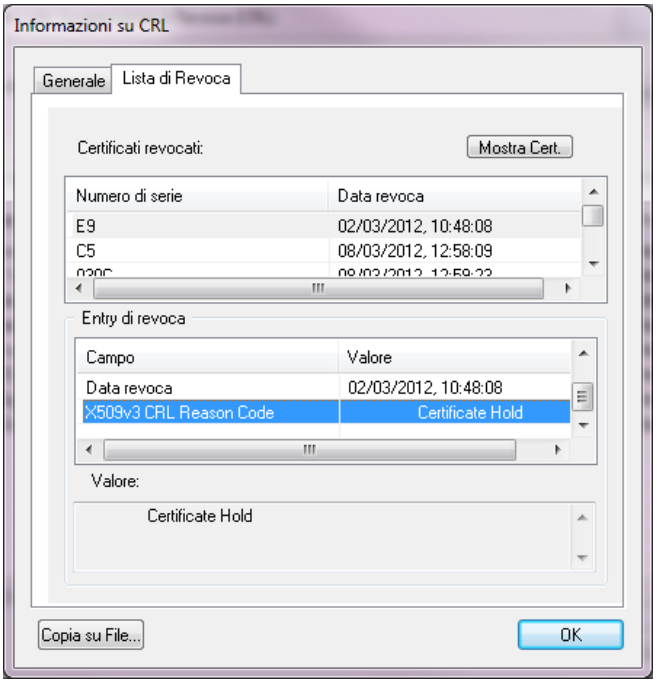
3.8.10 Modulo di visualizzazione di una Lista di Sospensione o Revoca

Questa finestra è organizzata in due cartelle, la prima della quale mostra le informazioni generali relative alla lista di revoca:



La tabella del primo riquadro mostra tutti gli elementi fondamentali della CRL, in particolare il nominativo della Certification Authority che l'ha emessa, la data effettiva di emissione, la data pianificata da Certificatore per l'emissione del prossimo aggiornamento.
Il riquadro inferiore mostra gli eventuali dettagli disponibili per l'elemento del primo riquadro correntemente selezionato

La seconda cartella mostra invece il contenuto effettivo della lista:



Si noti che una CRL contiene unicamente i numeri di serie come riferimenti ai certificati veri e propri, non contiene i certificati completi. Quindi è possibile sapere, dato un certificato, se esso è incluso nella lista (ricercandone il numero di serie), ma non è possibile conoscere le identità dei titolari di tutti i certificati revocati semplicemente disponendo della lista.

Tuttavia, se nel DB locale è presente un certificato corrispondente alla entry correntemente selezionata, il bottone **Mostra Certificato** lo apre per la visualizzazione.

Il riquadro superiore contiene la lista effettiva: una tabella le cui colonne rappresentano, rispettivamente, i numeri di serie dei certificati e la data di sospensione o revoca.

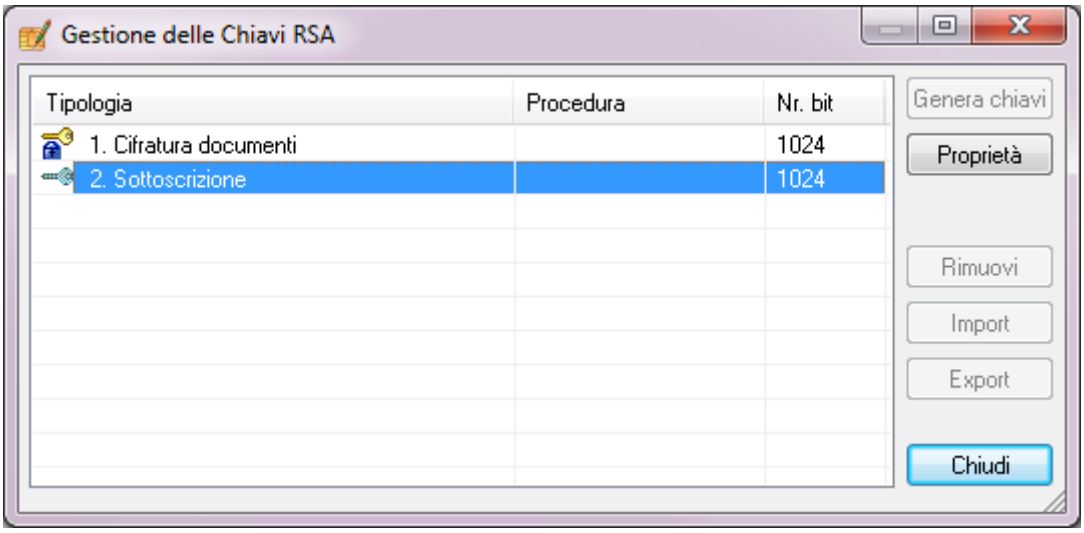
Il riquadro **Entry di revoca** mostra tutti i dettagli relativi alla riga della tabella superiore correntemente selezionata; numero di serie del certificato, data e ora della sospensione o revoca, il codice e descrizione dell'operazione impostato dal certificatore per quel certificato.

Il riquadro **Valore** mostra una ulteriore espansione del dettaglio correntemente selezionato nel riquadro delle entry di revoca.

Da entrambe le cartelle, con il bottone **Copia su File** è possibile esportare la CRL su un file esterno, con **OK** si chiude la finestra.

3.8.11 Modulo di gestione delle coppie di chiavi RSA

Questo modulo consente di operare sull'insieme di coppie di chiavi presenti in un dispositivo di firma:



La tabella mostra una riga per ogni coppia di chiavi disponibile nel dispositivo.

Per ognuna delle coppie di chiavi vengono visualizzate le seguenti informazioni:

- l'icona che rappresenta la tipologia
- la tipologia in esteso
- l'eventuale identificatore della procedura automatica (solo per le coppie di chiavi di sottoscrizione mediante procedura automatica): questa colonna è mantenuta per compatibilità con dispositivi di firma personalizzati con vecchie edizioni di DigitalSign
- la lunghezza delle chiavi, espressa in bit

Sono disponibili alcuni bottoni comando:

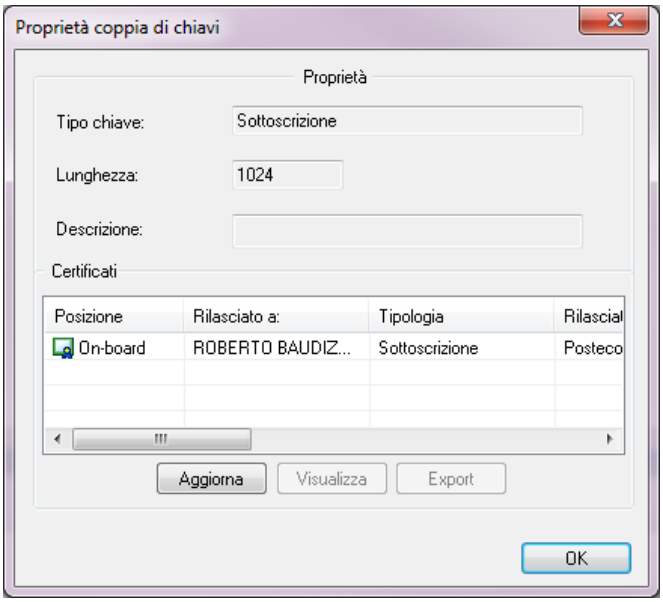
- **Genera chiavi -** conduce ad una finestra di dialogo che assiste alla creazione di una nuova coppia di chiavi. Questo comando è abilitato solo se si opera con un dispositivo che effettivamente consente la generazione.
- **Proprietà –** conduce ad una ulteriore finestra di dialogo che illustra proprietà di dettaglio della coppia di chiavi selezionata.
- **Import -** consente di importare da un file in formato PKCS#12 una coppia di chiavi di cifratura. In pratica è una operazione di *restore*, mentre l'export è assimilabile ad una operazione di *backup.*
  In generale questa funzione può non essere disponibile con le smartcard fornite dai Certificatori accreditati.
- **Export -** consente di esportare su un file in formato PKCS#12 una coppia di chiavi da utilizzare per la cifratura dei documenti (si noti che l'esportazione di una chiave privata per la firma digitale

sarebbe del tutto illegale). Lo scopo di questa operazione è quello di eseguire un backup (definito *key recovery*)al fine di non perdere la possibilità di decifrare documenti crittografati in caso di perdita o distruzione del dispositivo di firma che contiene le relative chiavi.
In generale questa funzione può non essere disponibile con le smartcard fornite dai Certificatori accreditati.
NOTA: una coppia di chiavi di cifratura potrà essere esportata solo se è stata creata fin dall'inizio con l'opzione di key recovery.

- **Chiudi** - chiude la finestra di dialogo

3.8.11.1 Proprietà di una coppia di chiavi

Viene mostrata una finestra di questo tipo:

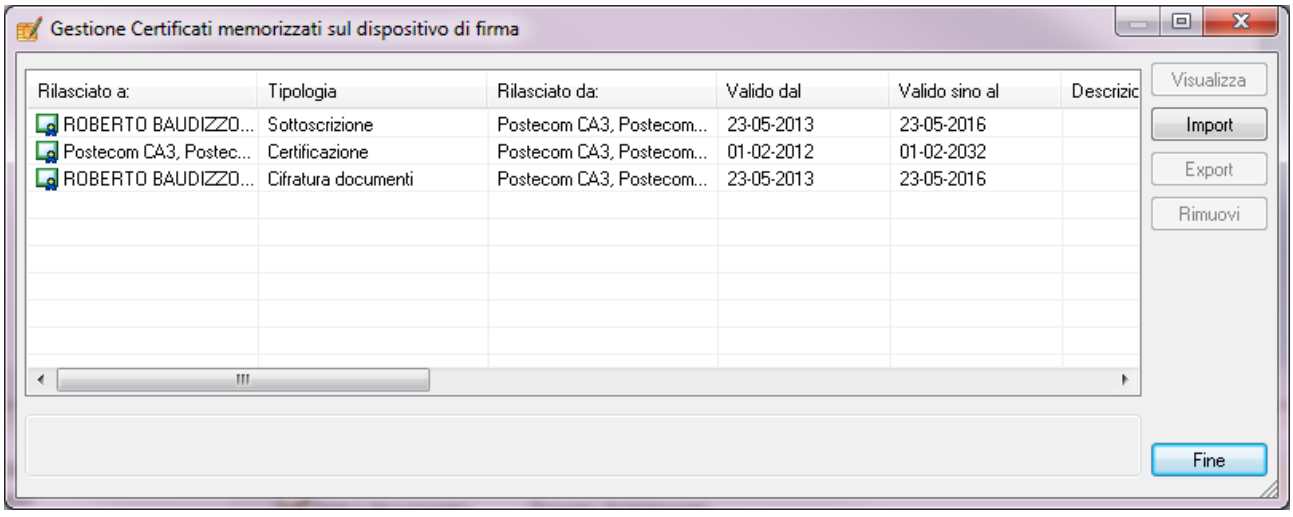


La tabella della finestra mostra il certificato o i certificati presenti nel sistema e che corrispondono alla coppia di chiavi.

- il bottone **Aggiorna** ripete la scansione degli archivi di DigitalSign alla ricerca dei certificati
- **Visualizza** apre la visualizzazione del certificato selezionato
- **Export** consente di esportare su un file esterno una copia del certificato selezionato

3.8.12 Modulo di Gestione dei Certificati 'on-board'

Questo modulo consente di esplorare i certificati contenuti a bordo del dispositivo di firma correntemente inserito.



Sono disponibili i seguenti bottoni comando:

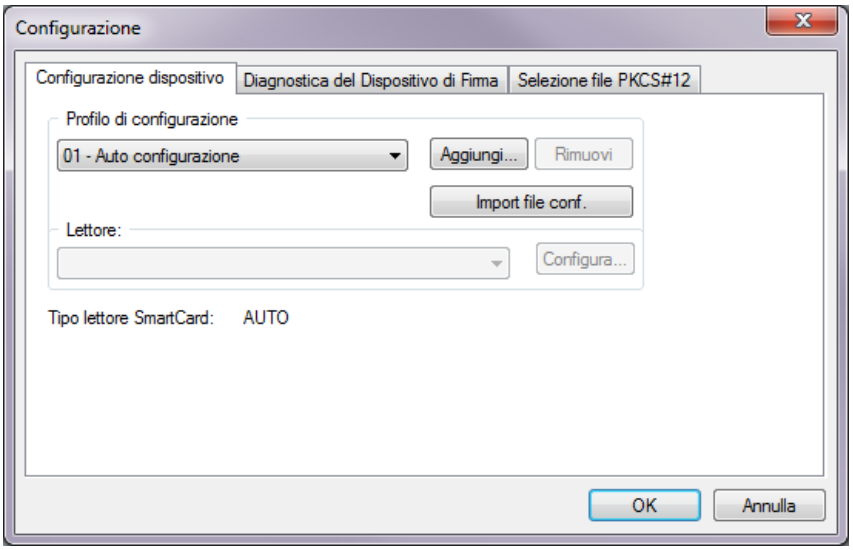
- **Visualizza** - per visualizzare il contenuto del certificato, tramite l'apposito visualizzatore (4.8.9)
- **Import** - per caricare nel dispositivo un certificato disponibile su file. L'effettiva disponibilità di questa funzione dipende dalla configurazione del particolare dispositivo
- **Export** - per esportare su un file esterno il certificato correntemente selezionato
- **Rimuovi** - per cancellare dalla memoria della smartcard il certificato selezionato. L'effettiva disponibilità di questa funzione dipende dalla configurazione del particolare dispositivo.

3.8.13 Modulo di Gestione della Configurazione del Dispositivo di Firma

DigitalSign può operare con una grande varietà di dispositivi di firma, che richiedono di essere correttamente interfacciati.
La gran parte delle smartcard e dei dispositivi di altro genere disponibili sul mercato – soprattutto quelli rilasciati dai Certificatori accreditati presso CNIPA – viene interfacciata attraverso lo standard PKCS#11; quindi DigitalSign deve mettere in funzione lo specifico modulo PKCS#11 (una .DLL) adatto per la particolare tipologia di smartcard, mentre nel secondo caso deve riconoscere correttamente il tipo di dispositivo ed attuare il corretto protocollo di comunicazione.

3.8.13.1 Auto-configurazione

Avendo a che fare con una smartcard già pronta all'uso, contenente chiavi e certificati, il modo più semplice di procedere è quello di attuare la configurazione automatica.



In questa modalità l'utente non deve fare nulla, ma solo lasciare che DigitalSign risolva automaticamente il problema della configurazione

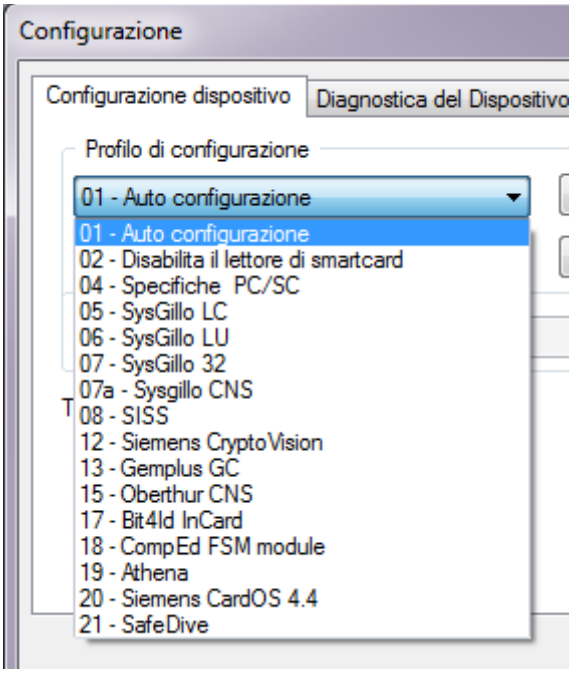
Il sistema opera come segue:

- all'avvio DigitalSign ricerca nel computer quali moduli PKCS#11 – tra quelli conosciuti da DigitalSign, elencati nel file **`devices.ini`** che si trova nella stessa cartella che ospita l'eseguibile – sono effettivamente presenti;
- al primo inserimento di una smartcard in uno dei lettori installati nel sistema DigitalSign tenta di leggerne i certificati contenuti in area pubblica (dove non è necessario disporre del PIN) attraverso i vari moduli PKCS#11 di cui dispone, fino a quando non ottiene un risultato positivo;
- una volta trovato il modulo PKCS#11 corretto DigitalSign registra l'associazione tra il codice identificativo del particolare tipo di smartcard (ATR) ed il modulo PKCS#11 che ha avuto successo nella lettura della carta, così da metterlo direttamente in uso la prossima volta che un dispositivo dello stesso tipo viene inserito in un lettore

Come si può intuire questa strategia può non andare a buon fine, oltre all'ovvio caso in cui la macchina non disponga del giusto modulo PKCS#11, nel caso in cui l'area pubblica del dispositivo non contenga alcun certificato.
Questo si verifica con le carte interamente vuote o con alcune smartcard i cui certificati sono memorizzati tutti in area privata invece che in area pubblica (ad oggi abbiamo esperienza di alcuni dispositivi di questo tipo rilasciati da Actalis), per i quali è richiesta la configurazione manuale.

3.8.13.2 Configurazione manuale

Se il modulo di configurazione automatica non riesce ad associare correttamente la smartcard a disposizione con un modulo PKCS#11 tra quelli installati nel sistema (può essere il caso di dispositivi vergini oppure di smartcard prive di certificati in area pubblica) è possibile eseguire la configurazione manuale, forzando DigitalSign a colloquiare con il dispositivo utilizzando una modalità ben determinata ed uno specifico lettore.

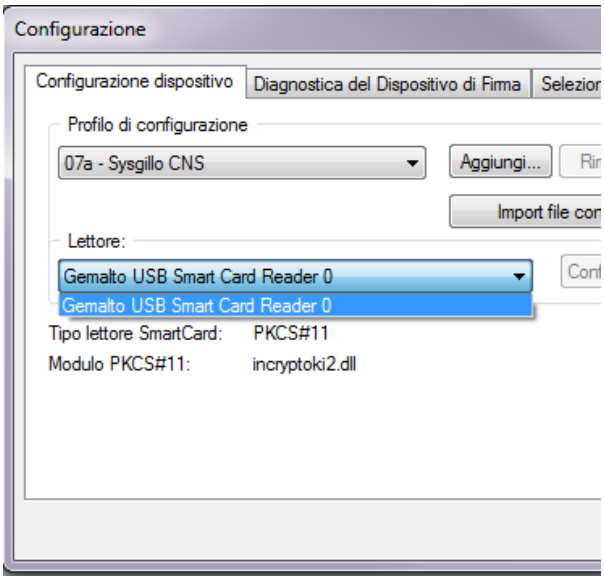


Innanzitutto occorre scegliere il modulo da impiegare, dalla lista completa di tutte le opzioni disponibili (cioè i moduli effettivamente installati sul computer).

Si noti che i primi elementi della lista sono speciali:

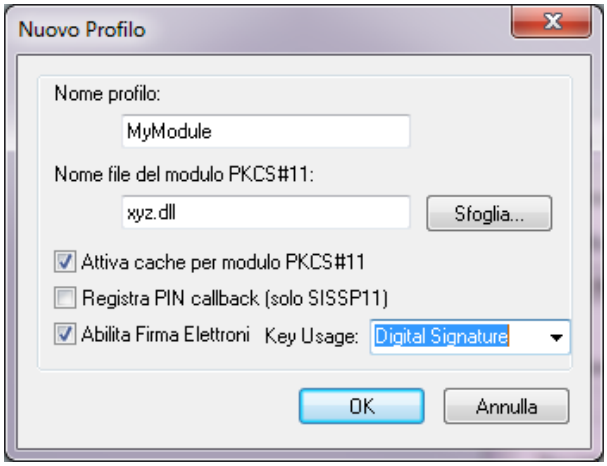
- 01 – **Auto configurazione** – attiva il riconoscimento automatico
- 02 – **Disabilita il lettore di smartcard** – predispone DigitalSign ad operare senza dispositivo di firma, evitando i messaggi di errore relativi all'assenza di un lettore
- 04 – **Specifiche PC/SC** – predispone DigitalSign ad interfacciare la smartcard in modalità APDU, senza alcuna intermediazione di moduli PKCS#11. In questa modalità sarà possibile utilizzare solo un set ristretto di dispositivi ben identificati

Dopo la selezione della modalità occorre anche specificare in quale lettore si trova il dispositivo, nel caso la macchina disponga di più di un lettore:



Qualora il dispositivo a disposizione richiedesse, per l'interfacciamento, un modulo PKCS#11 diverso da tutti quelli noti a DigitalSign, è comunque possibile aggiungere un nuovo profilo tramite il bottone **Aggiungi**, si veda la prossima sezione.

3.8.13.3 Aggiunta di un Profilo di Configurazione



Questa finestra consente di registrare in DigitalSign un nuovo profilo di configurazione per dispositivi PKCS#11.

Occorre assegnare al profilo un nome simbolico ed indicare il file .DLL che rappresenta l'interfaccia PKCS#11.

I tre checkbox sottostanti hanno il seguente significato:

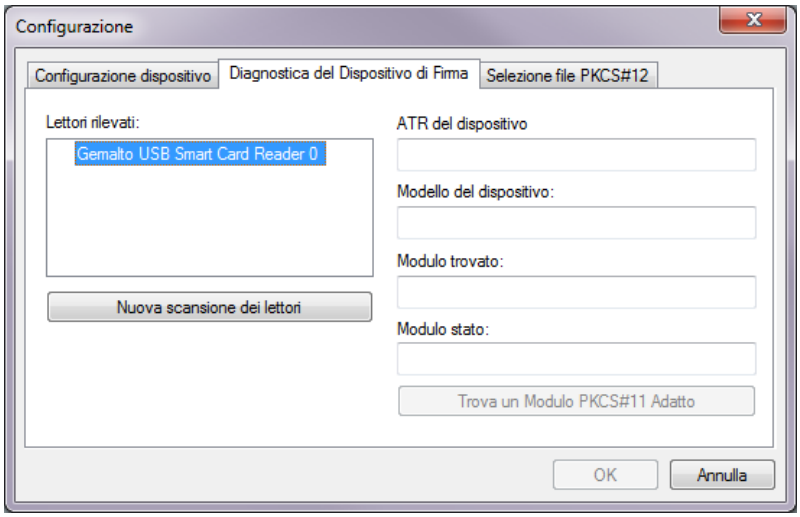
- **Attiva cache per il modulo PKCS#11** – se attivo fa sì che DigitalSign, una volta collegato positivamente un dispositivo a questo modulo, registri l'associazione mediante l'ATR del dispositivo stesso, così che successivi inserimenti di dispositivi dello stesso tipo colleghino direttamente questo modulo se è attiva la modalità di auto-configurazione.
  In taluni casi può essere opportuno disabilitare questa opzione (per esempio con smartcard che hanno lo stesso ATR ma vengono personalizzati tramite diversi layer: è necessario lasciare che DigitalSign trovi il modulo giusto tramite la lettura sperimentale dei certificati di bordo)
- **Registra PIN callback** – questa è una funzione speciale, riservata ad uno specifico modulo (SISSP11) e consente di gestire in modo automatico il PIN di firma, evitando la doppia richiesta del PIN. Si raccomanda di non attivare questa opzione se non su indicazioni del fornitore
- **Abilita Attestazione** – questa opzione istruisce il sistema ad abilitare, per i dispositivi di firma interfacciati per tramite di questo modulo, la funzione di Firma Elettronica (firma debole).

In caso di abilitazione di questo checkbox è anche necessario specificare quale *"key usage"* devono avere i certificati da usare per questo scopo. Si raccomanda di usare **Digital Signature**.

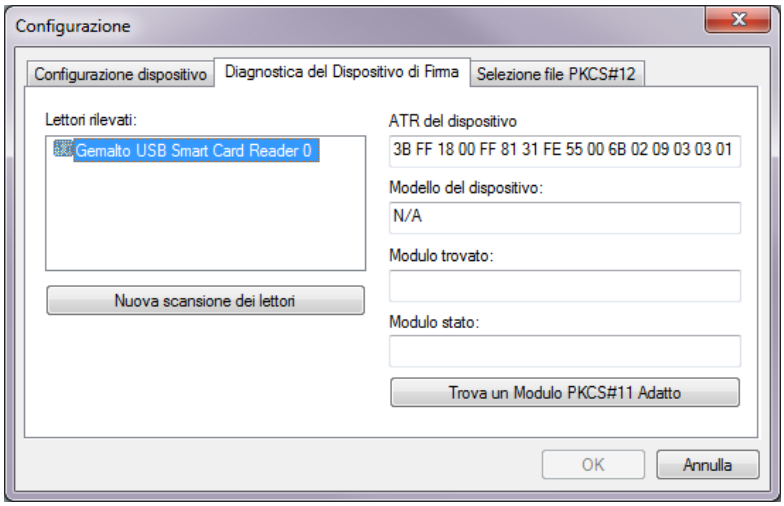
3.8.13.4 Diagnostica del dispositivo

Questo pannello consente di controllare i passi svolti da DigitalSign nella ricerca automatica di un modulo PKCS#11 adatto ad interfacciare un dispositivo di firma.

Se nessun dispositivo è inserito in un lettore il pannello può presentarsi come in figura:

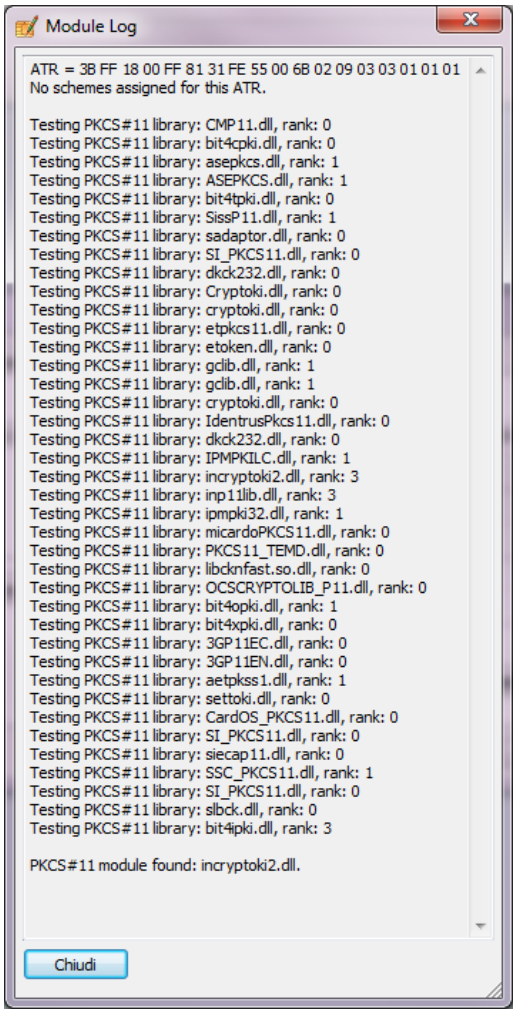


Il bottone **Nuova scansione dei lettori** forza il sistema a rileggere lo stato dei lettori, aggiornando la lista. Ma normalmente è sufficiente inserire una smartcard in un lettore per veder aggiornare la finestra in questo modo:

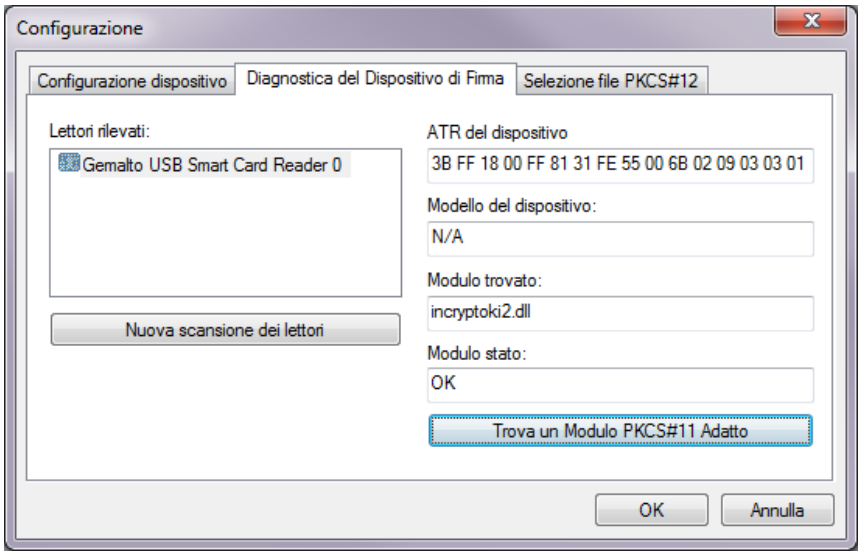


Il simbolo della smartcard appare accanto al nome del lettore, mentre nel riquadro a destra compare il codice ATR (*Answer To Reset*) del dispositivo.
Talvolta è disponibile anche una denominazione del modello del dispositivo.

Agendo sul bottone **Trova un modulo PKCS#11 adatto** si avvia il processo di tentativi illustrato in precedenza; se l'ATR del dispositivo in questione non era mai stato incontrato e se si dispone di diversi moduli li vedremo testare uno per uno.
Alla fine del procedimento il sistema presenta una finestra di log, più o meno ricca in funzinoe del numero di moduli PKCS#11 effettivamente installati:


Module Log
ATR = 3B FF 18 00 FF 81 31 FE 55 00 6B 02 09 03 03 01 01 01
No schemes assigned for this ATR.
Testing PKCS#11 library: CMP11.dll, rank: 0
Testing PKCS#11 library: bit4cpki.dll, rank: 0
Testing PKCS#11 library: asepkcs.dll, rank: 1
Testing PKCS#11 library: ASEPKCS.dll, rank: 1
Testing PKCS#11 library: bit4tpki.dll, rank: 0
Testing PKCS#11 library: SissP11.dll, rank: 1
Testing PKCS#11 library: sadaptor.dll, rank: 0
Testing PKCS#11 library: SI_PKCS11.dll, rank: 0
Testing PKCS#11 library: dkck232.dll, rank: 0
Testing PKCS#11 library: Cryptoki.dll, rank: 0
Testing PKCS#11 library: cryptoki.dll, rank: 0
Testing PKCS#11 library: etpkcs11.dll, rank: 0
Testing PKCS#11 library: etoken.dll, rank: 0
Testing PKCS#11 library: gclib.dll, rank: 1
Testing PKCS#11 library: gclib.dll, rank: 1
Testing PKCS#11 library: cryptoki.dll, rank: 0
Testing PKCS#11 library: IdentrusPkcs11.dll, rank: 0
Testing PKCS#11 library: dkck232.dll, rank: 0
Testing PKCS#11 library: IPMPKILC.dll, rank: 1
Testing PKCS#11 library: incryptoki2.dll, rank: 3
Testing PKCS#11 library: inp11lib.dll, rank: 3
Testing PKCS#11 library: ipmpki32.dll, rank: 1
Testing PKCS#11 library: micardoPKCS11.dll, rank: 0
Testing PKCS#11 library: PKCS11_TEMD.dll, rank: 0
Testing PKCS#11 library: libcknfast.so.dll, rank: 0
Testing PKCS#11 library: OCSCRYPTOLIB_P11.dll, rank: 0
Testing PKCS#11 library: bit4opki.dll, rank: 1
Testing PKCS#11 library: bit4xpki.dll, rank: 0
Testing PKCS#11 library: 3GP11EC.dll, rank: 0
Testing PKCS#11 library: 3GP11EN.dll, rank: 0
Testing PKCS#11 library: aetpkss1.dll, rank: 1
Testing PKCS#11 library: settoki.dll, rank: 0
Testing PKCS#11 library: CardOS_PKCS11.dll, rank: 0
Testing PKCS#11 library: SI_PKCS11.dll, rank: 0
Testing PKCS#11 library: siecap11.dll, rank: 0
Testing PKCS#11 library: SSC_PKCS11.dll, rank: 1
Testing PKCS#11 library: SI_PKCS11.dll, rank: 0
Testing PKCS#11 library: slbck.dll, rank: 0
Testing PKCS#11 library: bit4ipki.dll, rank: 3
PKCS#11 module found: incryptoki2.dll.
Chiudi

Chiudendo la finestra dovremmo vedere il risultato:

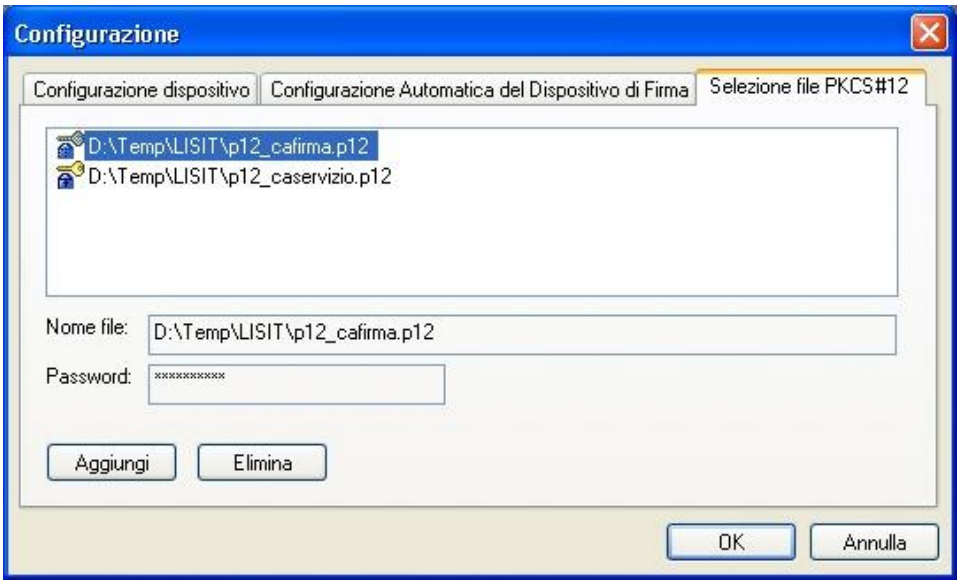


3.8.13.5 Caricamento file PKCS#12

Alcune funzioni di DigitalSign possono essere eseguite anche con chiavi RSA gestite in software, non residenti su smartcard; attualmente tale opzione è disponibile soltanto per le operazioni di decifratura documenti.

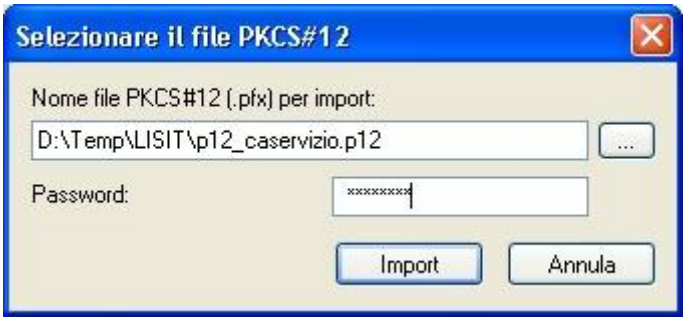
Se per le chiavi private di firma digitale è essenziale, a fini di sicurezza, che in nessun caso sia possibile l'esportazione o la duplicazione, per le chiavi private destinate alla decifratura di documenti è importante poter disporre del backup delle chiavi private.
Un documento cifrato diventa infatti del tutto illeggibile in caso di perdita o malfunzionamento della smartcard che contiene l'unica chiave privata idonea a decifrarlo. Quindi è prassi piuttosto comune usare per questo scopo delle chiavi private con opzione di key-recovery, che vengono esportate su file in formato PKCS#12 (sono file a loro volta cifrati e protetti con password, contenenti la chiave privata ed il relativo certificato).
Allorché si intende usare una chiave così esportata sarà possibile importarla su una nuova smartcard, ma è altresì possibile usarla direttamente dal file PKCS#12.

Questo modulo consente appunto l'utilizzo diretto di chiavi e certificati contenuti in file PKCS#12.



DigitalSign può caricare le chiavi ed i certificati di uno o più file PKCS#12 e gestirli come se fossero contenuti nella smartcard correntemente inserita.
A tal fine è necessario registrare i file PKCS#12 desiderati attraverso questo modulo, che presenta tutti i file correntemente registrati.

- Con il bottone **Elimina** si rimuove la registrazione del file correntemente selezionato
- Con il bottone **Aggiungi** si passa ad una ulteriore finestra:



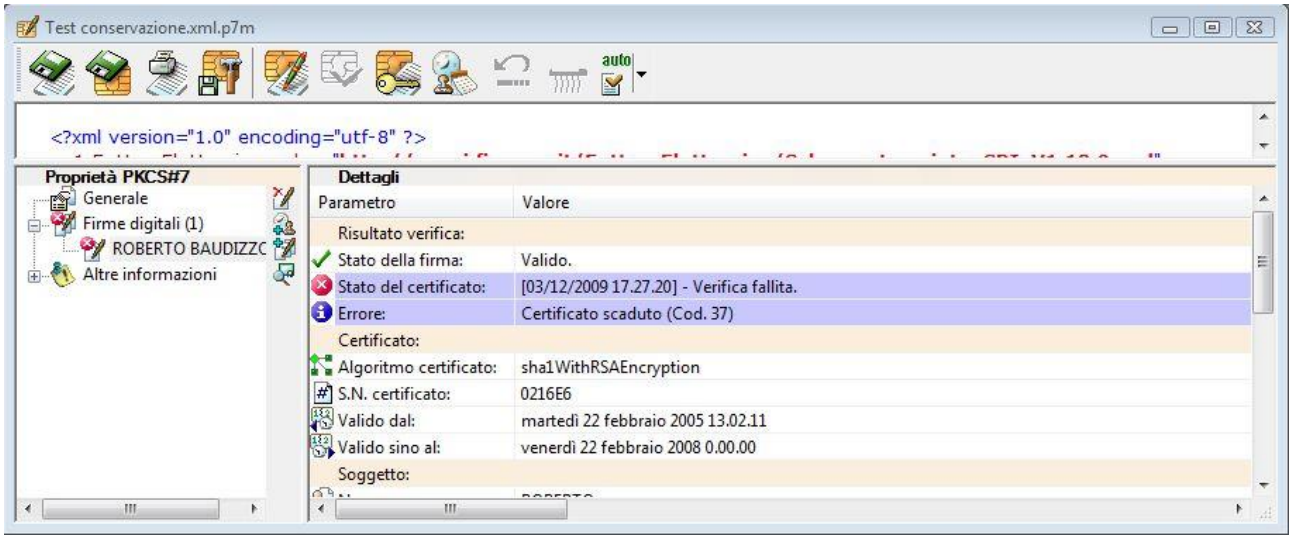
Da qui è possibile selezionare il file da importare e fornire la password per accedere al contenuto del file stesso.
Con **Import** si conferma la registrazione del file, con **Annulla** si torna alla schermata precedente.

NOTA IMPORTANTE: si ribadisce che le chiavi ed i certificati importati dai file PKCS#12 specificati per tramite di questo ambiente di configurazione vengono utilizzati da DigitalSign – limitatamente alla funzione di decifratura documenti – come se le stesse chiavi e certificati fossero presenti nella smartcard correntemente inserita.
Questo significa anche che se nessuna smartcard è inserita, non sarà possibile usare nemmeno gli oggetti software letti dai file PKCS#12: questo perché l'architettura interna di DigitalSign mette in funzione certe strutture solo quando un dispositivo di firma è correttamente interfacciato.

3.8.14 Verifica alla Data

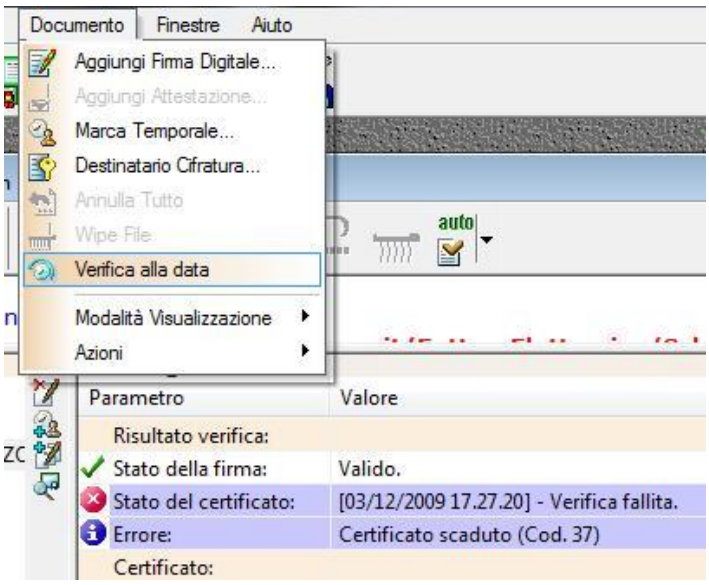
Con il 3 Dicembre 2009 è entrata in vigore una nuova modalità di emissione delle liste di sospensione e revoca (si veda la sezione sulla verifica delle firme digitali), che ora non vengono più depurate delle informazioni di revoca relativa a certificati di cui sia ormai terminata la validità nominale.
Grazie a questa novità è possibile, solo esaminando la CRL attuale, determinare se un certificato fosse indenne da provvedimenti di sospensione o revoca in una qualsiasi data compresa nel periodo di validità nominale (con l'esclusione di certificati comunque scaduti prima del 3/12/2009).
DigitalSign consente dunque di effettuare verifiche di firme digitali riferite ad una data qualsiasi, non quella attuale.

Normalmente, aprendo un documento firmato (non corredato di marca temporale) e navigando nel pannello delle proprietà sino ad espandere una particolare firma, vedremo qualcosa del genere:

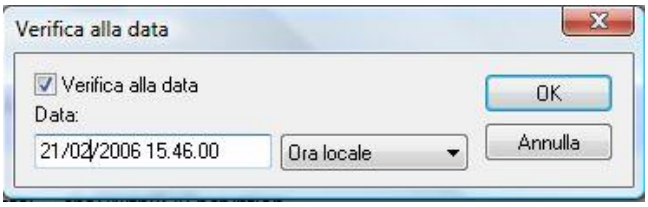


Come si vede la riga relativa allo **Stato del Certificato** riporta tra parentesi quadre una data ed un'ora di riferimento (nella figura 3/12/2009, ore 17:27). In generale quella è la data ed ora attuale.
Nel caso in figura la verifica è "non superata" perché allo stato attuale il certificato risulta scaduto.

Se a questo punto vogliamo sapere se il certificato fosse valido in un'epoca passata possiamo utilizzare la funzione di **Verifica alla Data:**

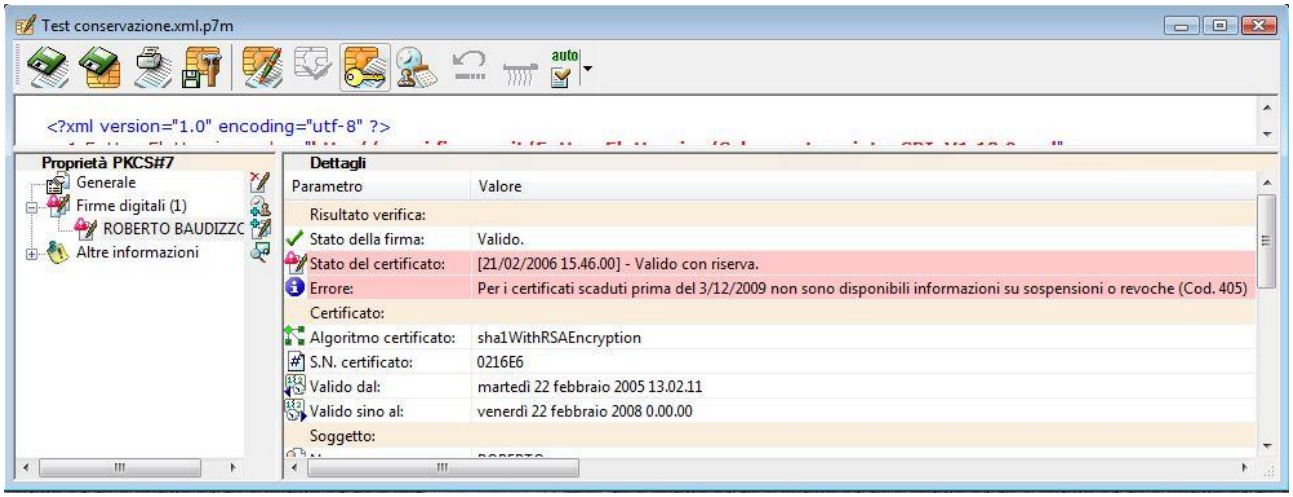


Verrà visualizzata questa piccola finestra di dialogo:



L'utente sarà invitato a selezionare il checkbox per attivare la verifica ad una data diversa da quella attuale, quindi ad inserire la data ed ora di riferimento (eventualmente distinguendo, liberamente, tra ora locale e UTC). Nel nostro caso inseriremo una data anteriore a quella di scadenza del certificato in questione.

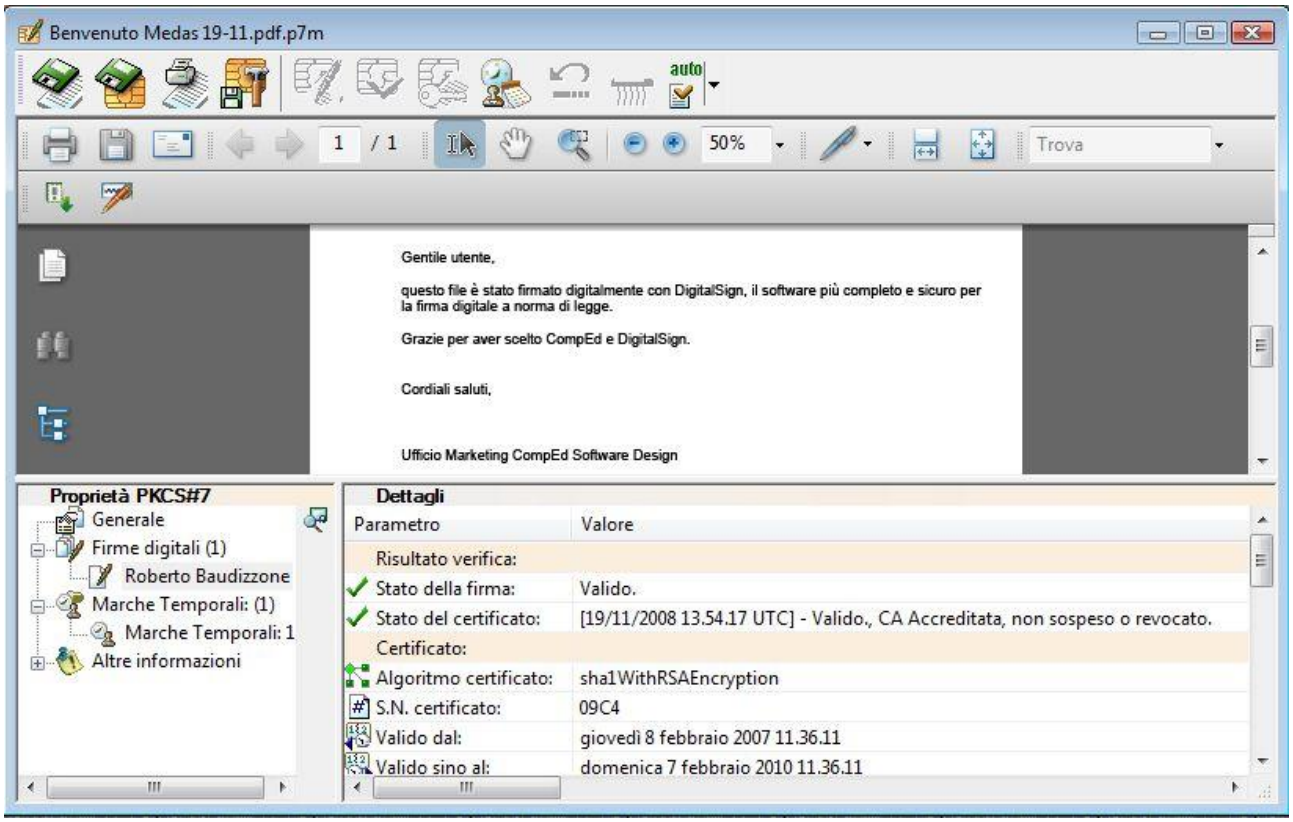
Una volta premuto OK DigitalSign aggiorna i propri pannelli e mostra il risultato della verifica ricalcolato alla data indicata dall'utente:



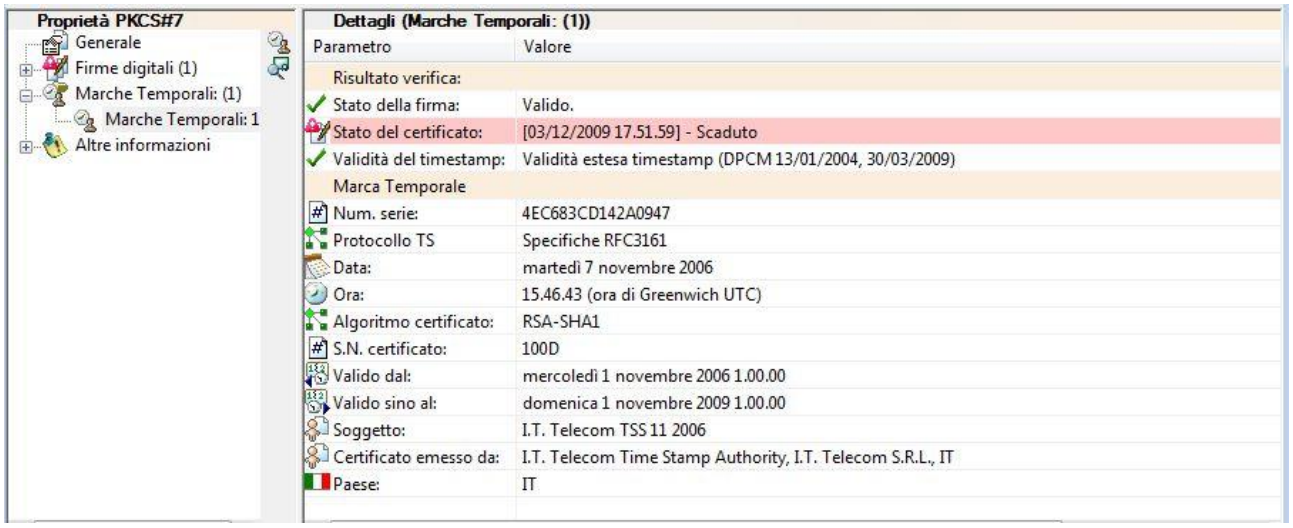
Questa immagine mostra un effetto particolare, che in quest'epoca sarà molto comune e tenderà poi a diventare più raro.
Come detto, le CRL contengono obbligatoriamente le informazioni di sospensioni e revoca anche per certificati ormai scaduti solo dal 3 dicembre 2009. Quindi, se il certificato in corso di analisi è scaduto prima di tale data e la CRL non contiene alcun riferimento a quel certificato, non è possibile stabilire con certezza che effettivamente non fosse mai avvenuta una sospensione o revoca. Quindi, in un caso del genere, DigitalSign dichiarerà "valido con riserva" e segnala un opportuno messaggio di warning.

3.8.14.1 Verifica di documenti marcati temporalmente

Il meccanismo di *Verifica alla Data* è particolarmente utile quando si verifichino documenti firmati e marcati temporalmente.
In questo caso DigitalSign esegue automaticamente la verifica riferita alla data ed ora corrispondenti alla marca temporale, presentando con un solo colpo d'occhio l'effettivo stato di validità di un documento marcato temporalmente:


Benvenuto Medas 19-11.pdf.p7m
Gentile utente,
questo file è stato firmato digitalmente con DigitalSign, il software più completo e sicuro per la firma digitale a norma di legge.
Grazie per aver scelto CompEd e DigitalSign.
Cordiali saluti,
Ufficio Marketing CompEd Software Design
Proprietà PKCS#7
Generale
Firme digitali (1)
Roberto Baudizzone
Marche Temporali: (1)
Marche Temporali: 1
Altre informazioni
Dettagli
Parametro
Valore
Risultato verifica:
Stato della firma: Valido.
Stato del certificato: [19/11/2008 13.54.17 UTC] - Valido., CA Accreditata, non sospeso o revocato.
Certificato:
Algoritmo certificato: sha1WithRSAEncryption
S.N. certificato: 09C4
Valido dal: giovedì 8 febbraio 2007 11.36.11
Valido sino al: domenica 7 febbraio 2010 11.36.11

Se andiamo poi ad aprire un documento marcato temporalmente tempo addietro, tanto che il relativo certificato (della marca temporale) sia già scaduto, vedremo che DigitalSign considera comunque valida la marca temporale tenendo conto del periodo di validità stabilito dalla normativa, in base alla configurazione delle opzioni di security, sezione firma e verifica:


Proprietà PKCS#7
Generale
Firme digitali (1)
Marche Temporali: (1)
Marche Temporali: 1
Altre informazioni
Dettagli (Marche Temporali: (1))
Parametro
Valore
Risultato verifica:
Stato della firma: Valido.
Stato del certificato: [03/12/2009 17.51.59] - Scaduto
Validità del timestamp: Validità estesa timestamp (DPCM 13/01/2004, 30/03/2009)
Marca Temporale
Num. serie: 4EC683CD142A0947
Protocollo TS Specifiche RFC3161
Data: martedì 7 novembre 2006
Ora: 15.46.43 (ora di Greenwich UTC)
Algoritmo certificato: RSA-SHA1
S.N. certificato: 100D
Valido dal: mercoledì 1 novembre 2006 1.00.00
Valido sino al: domenica 1 novembre 2009 1.00.00
Soggetto: I.T. Telecom TSS 11 2006
Certificato emesso da: I.T. Telecom Time Stamp Authority, I.T. Telecom S.R.L., IT
Paese: IT

3.9 Appendici

3.9.1 Interfacciamento dei dispositivi di firma

DigitalSign 3.1 è in grado di supportare lo standard PKCS#11 per interfacciare dispositivi per la creazione di firme digitali.

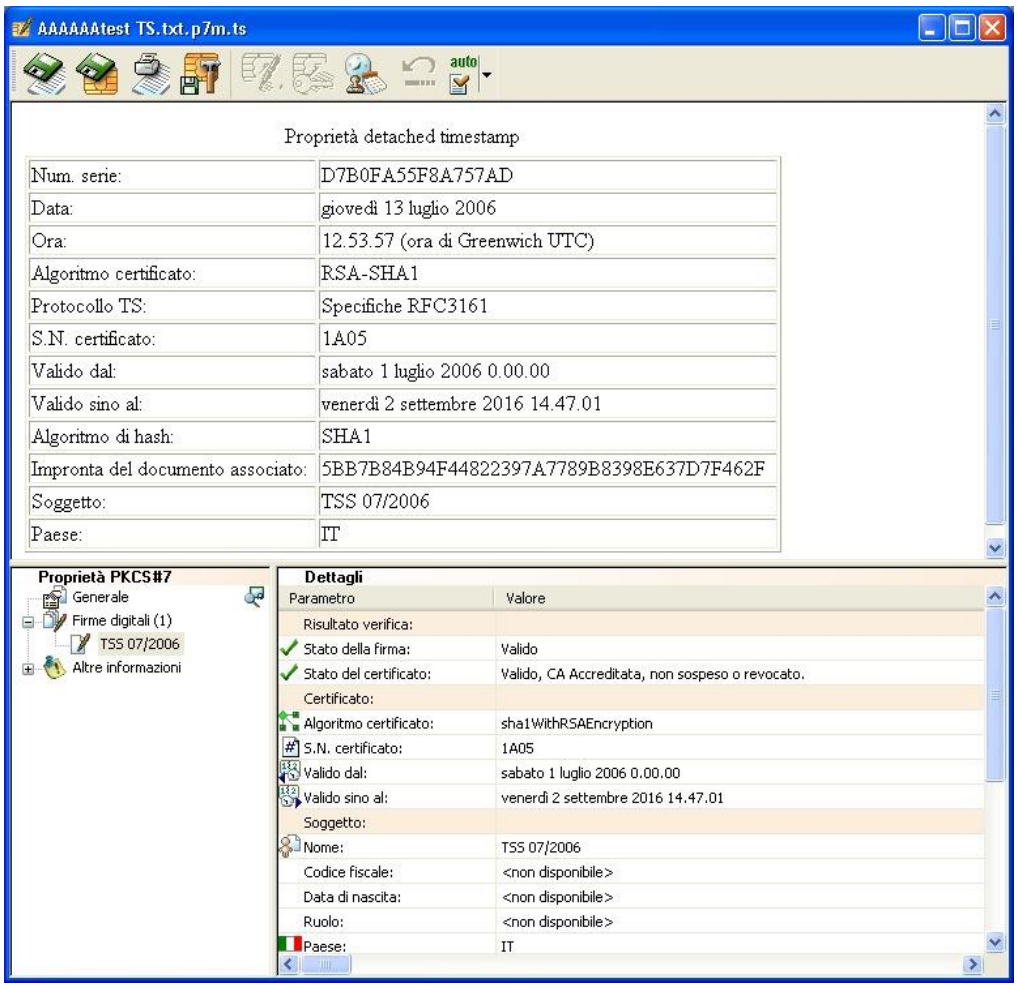
Poiché lo standard PKCS#11 non è sufficientemente rigoroso da assicurare il funzionamento corretto in tutti i casi possibili, non è possibile assicurare preventivamente che qualunque dispositivo “PKCS#11 compatibile” possa funzionare pienamente con DigitalSign.
Tuttavia l’esperienza accumulata nel settore ci permette di dichiarare che allo stato DigitalSign può utilizzare tutti i dispositivi di firma PKCS#11 rilasciati dai Certificatori Accreditati, in quanto non abbiamo notizia di incompatibilità.
D’altronde non possiamo escludere che in qualsiasi momento venga immesso sul mercato un dispositivo differente, che potrebbe porre problemi e richiedere un intervento di adattamento.
Inoltre l’interfaccia PKCS#11 di ciascun dispositivo consiste di un modulo software fornito con la smartcard (o messo a disposizione dal Certificatore che rilascia la carta stessa); tale modulo va installato sulla macchina, rispettandone le restrizioni e i limiti di compatibilità.
Anche per tutte queste ragioni l’effettiva operatività di un particolare dispositivo con DigitalSign non può essere garantita a priori e va verificata a cura dell’utente.

3.9.2 Marche temporali: contenuto e modalità di associazione ai documenti

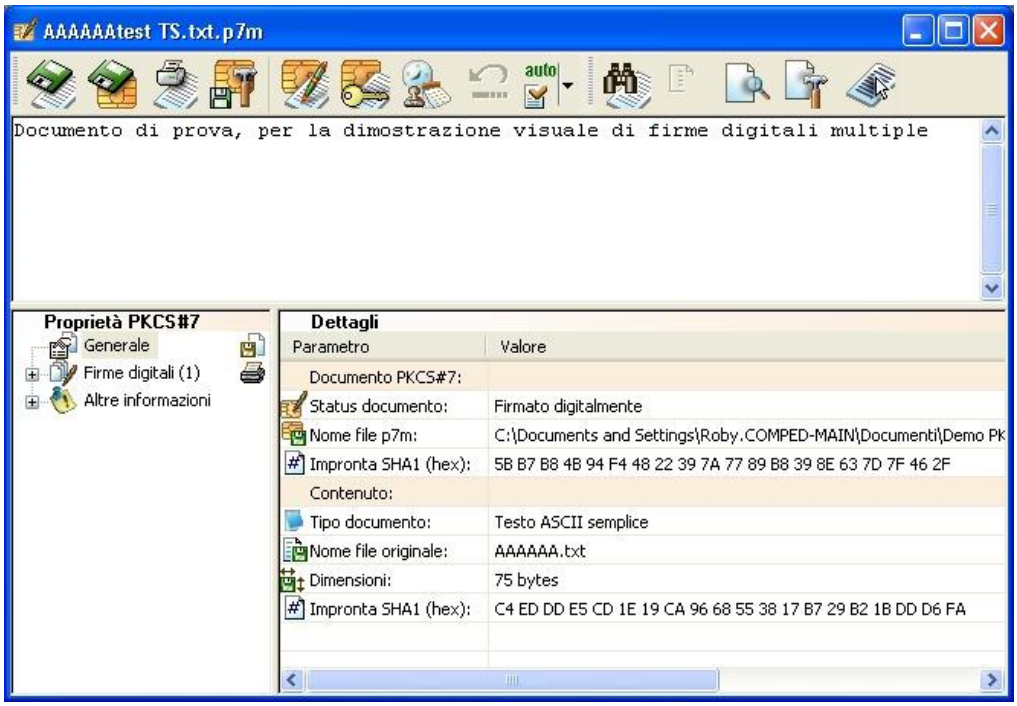
Una marca temporale è di per sé un documento informatico firmato digitalmente.
I fornitori del Servizio di Marcatura Temporale accreditati presso AgID erogano tali marche temporali in accordo con le specifiche descritte nella Deliberazione CNIPA 45/2009.

Non va però dimenticato che una marca temporale ha poco significato di per sé, mentre è fondamentale il suo significato quando è associata ad un altro documento informatico: poiché la marca temporale contiene l’impronta del documento a cui è associata serve a dimostrare l’esistenza di tale documento all’istante testimoniato dalla marca temporale.

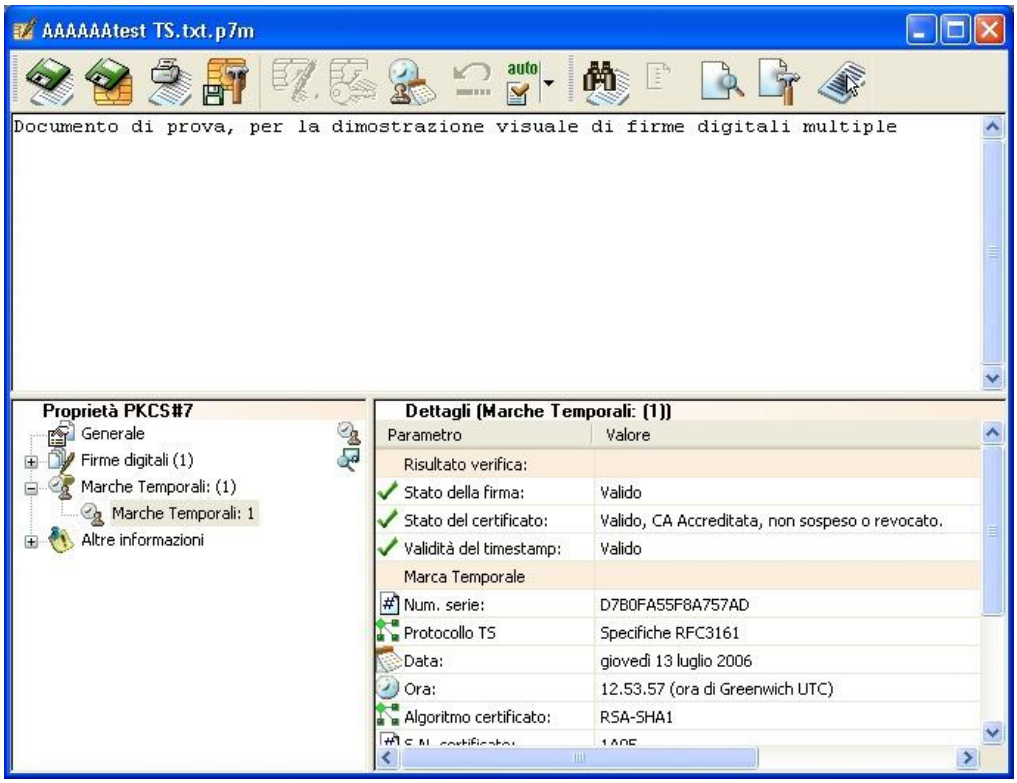
La figura qui sotto mostra il contenuto di una marca temporale esaminata separatamente dal documento cui è riferita:



Quest'altra mostra il documento a cui la marca era stata associata. Si noti la coincidenza dei valori di impronta:



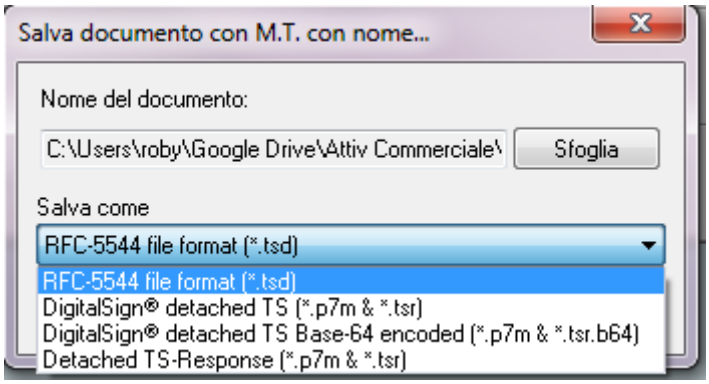
Naturalmente sarebbe troppo macchinoso per l'utente verificare visivamente l'identità dell'impronta del documento e quello dell'impronta oggetto della marca temporale; per questo DigitalSign apre la coppia di documenti insieme, mostrando il documento marcato temporalmente:



Ma per ottenere un tale obiettivo occorre individuare una modalità per associare i due oggetti.
Le regole tecniche contenute nella Deliberazione CNIPA 45/2009 finalmente individuano un formato standard (RFC 5544) per associare un documento ad una marca temporale ed indicano anche una modalità per associare direttamente una marca temporale ad una firma (CAdES-T).

La seconda modalità è “trasparente” rispetto alla necessità di memorizzazione, perché la marca temporale è integrate nella busta crittografica .p7m.

La prima modalità, invece, prevede che si produca un file .tsd che incorpora i due oggetti originariamente separati (documento e marca).
Allo stato DigitalSign consente ancora di salvare i documenti marcati temporalmente nei formati proprietari utilizzati fino allentata in vigore della Deliberazione CNIPA 45/2009 (Settembre 2010), ma si raccomanda senz’altro di utilizzare il nuovo formato.


Salva documento con M.T. con nome...
Nome del documento:
C:\Users\roby\Google Drive\Attiv Commerciale\
Sfoglia
Salva come
RFC-5544 file format (*.tsd)
RFC-5544 file format (*.tsd)
DigitalSign® detached TS (*.p7m & *.tsr)
DigitalSign® detached TS Base-64 encoded (*.p7m & *.tsr.b64)
Detached TS-Response (*.p7m & *.tsr)

Le diverse modalità supportate sono le seguenti:

- **Modalità “RFC-5544 file format (*.p7m.tsd)**
  È lo standard previsto dalle regole tecniche 2009 per rappresentare un documento firmato (CAdES-BES) ed una marca temporale detached che copra l’intero documento.

- **Modalità "DigitalSign detached TS (*.p7m & *.tsr)"**
  Il documento e la marca temporale vengono memorizzati separatamente, come due file PKCS#7 codificati in DER.
  La *naming convention* adottata prevede per il documento vero e proprio la denominazione prescritta da AgID (es. mydoc.pdf.p7m) e per la marca temporale lo stesso nome con l'ulteriore estensione .tsr (es. mydoc.pdf.p7m.ts).
  Poiché i due file hanno lo stesso nome DigitalSign trova immediatamente la marca temporale al momento di aprire il file principale (ovviamente a condizione che i due file siano memorizzati nella stessa cartella.

- **Modalità "DigitalSign detached TS Base-64 encoded (*.p7m & *ts.b64)"**
  Del tutto analoga alla modalità precedente, ma entrambi i file sono espressi in formato base64. La marca temporale reca l'estensione specifica (per chiarezza), mentre il documento mantiene l'estensione .p7m in ossequio alle linee guida di CNIPA.

3.9.3 La cifratura dei contenuti in DigitalSign

Con la versione 5.0 DigitalSign abbandona l’approccio di integrare la cifratura dei documenti a livello della stessa busta crittografica CAdES che ospita anche le firme, in favore di una cifratura a due livelli di busta.
Questo approccio è meno elegante e sofisticato, ma supportato da più prodotti, pertanto abbiamo ritenuto di sollevare l’utente da una scelta non sempre ovvia che comporta l rischio di difficoltà a livello di interoperabilità.

Pertanto, se si decide di firmare un documento di tipo .p7m, si otterrà un risultato di tipo .p7m.p7e

La cifratura del contenuto di un documento, in DigitalSign, avviene dunque all’interno di una struttura PKCS#7 e può riguardare documenti firmati o privi di firma.

L’algoritmo di cifratura è di tipo misto:

- innanzitutto viene generata, con una procedimento casuale, una chiave di crittografia simmetrica
- la chiave simmetrica viene usata per cifrare il contenuto del documento

- la stessa chiave simmetrica viene poi cifrata a sua volta usando la chiave pubblica del destinatario; nel caso siano previsti più destinatari questa operazione viene ripetuta per ciascuno di essi. La chiave pubblica di ogni destinatario viene estratta dal relativo certificato (si ricorda che la selezione dei destinatari di cifratura avviene selezionandone i relativi certificati)
- il documento viene confezionato inserendo nella busta PKCS#7 il documento cifrato e tutte le copie cifrate della chiave simmetrica

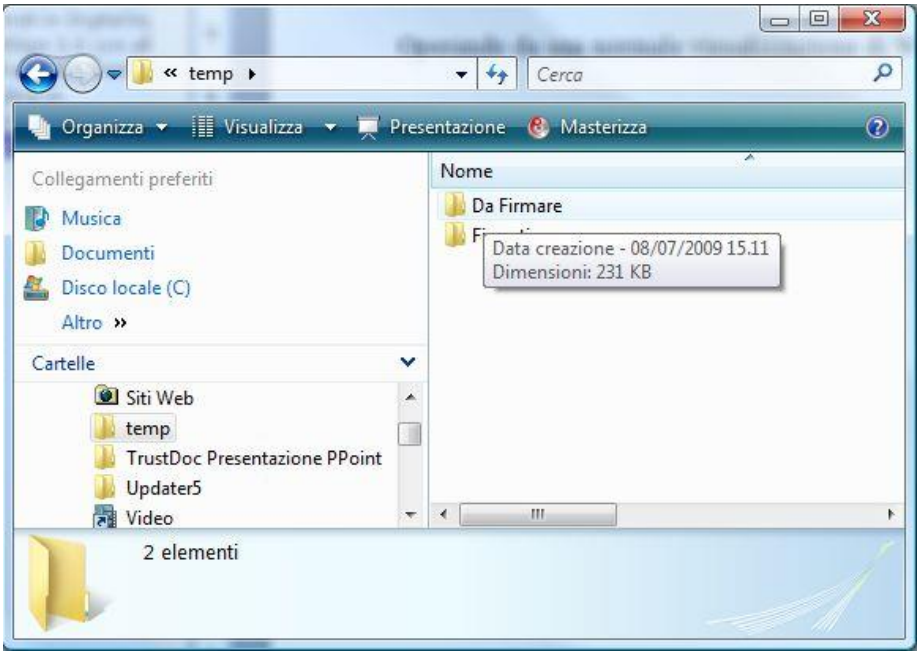
Il destinatario potrà usare la propria chiave privata per decifrare la chiave simmetrica e quindi potrà usare quest'ultima per decodificare il documento.

NOTA: la crittografia simmetrica è basata sull'algoritmo selezionato a livello di opzioni tra una lista molto nutrita di alternative.
La crittografia asimmetrica attuata sulla chiave simmetrica viene invece eseguita con l'algoritmo supportato dalla chiave pubblica disponibile nel certificato prescelto (di solito RSA 1024 o 2048)..

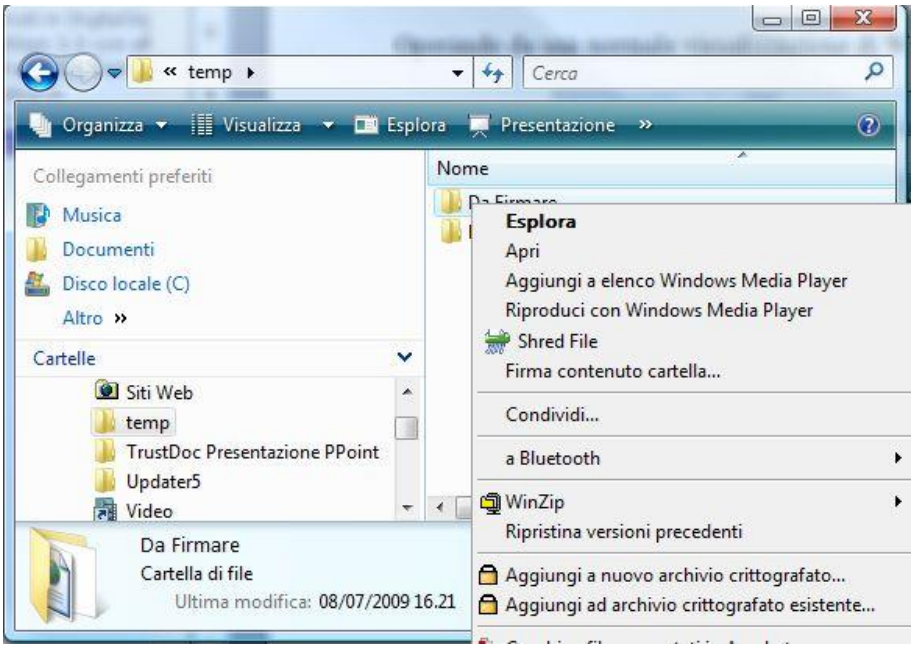
3.9.4 Firma semiautomatica dalla *shell* di Windows

Se a livello di Opzioni -> Associazioni viene opportunamente abilitata l'opzione **Tutti gli altri tipi** (si veda la sezione relativa), DigitalSign offrirà dalla *shell* di Windows la possibilità di attivare direttamente la firma semiautomatica di tutti i documenti presenti in una data cartella senza passare per la normale interfaccia di DigitalSign.

Operando da una normale visualizzazione di Windows Explorer, si localizzi la cartella su cui agire:



Quindi, facendo click con il tasto destro del mouse sulla cartella (nel nostro caso Da Firmare) si vedrà un menu proprio di Windows. Il contenuto effettivo del nostro menu dipende dalle applicazioni che abbiamo installato:



A noi adesso interessa la voce **Firma contenuto cartella**: agendo su questa opzione si lancerà DigitalSign (se non è già attivo) e si passa automaticamente alla condizione corrispondente alla voce del menu **File -> Firma contenuto cartella**, cui è dedicata una sezione di questa guida.